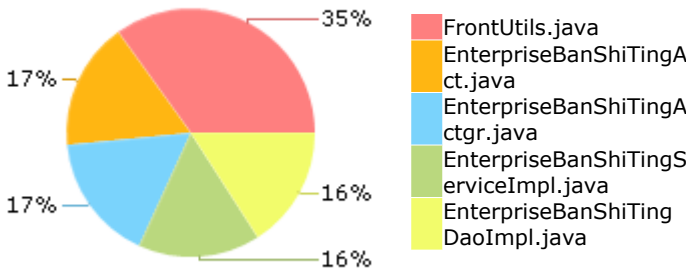
baoanwangban-2 扫描报告

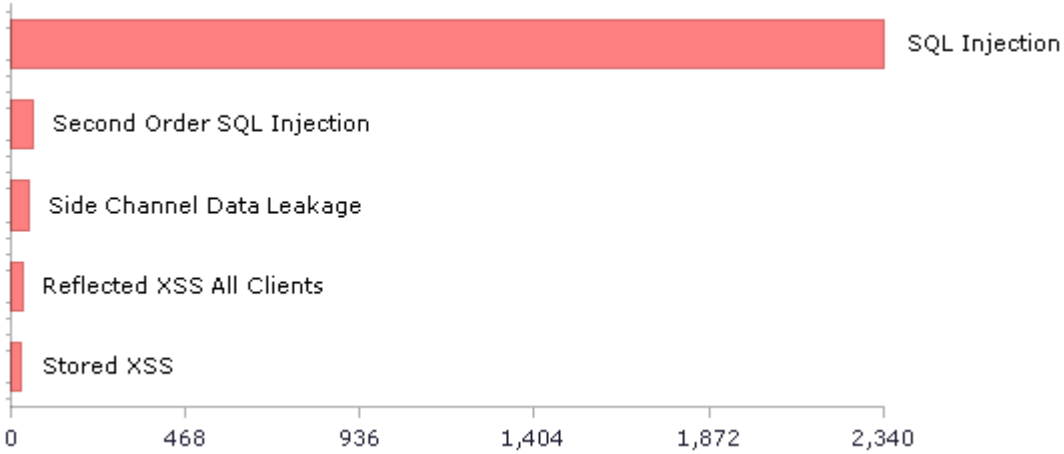
專案名稱	baoanwangban-2
扫描开始	2016年3月23日 10:40:01
預設集合	ZERO
扫描时间	01h:22m:55s
掃描程式行數	743,307
被扫描的文件	3826
报告创建时间	2016年3月23日 16:27:28
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188
团队	Users
Checkmarx版本	7.1.6 HF2
扫描类别	完整的
来源	LocalPath
缺陷密度	3/1000 (漏洞/LOC)
扫描注释	

扫描结果汇总

最易受攻击的文件



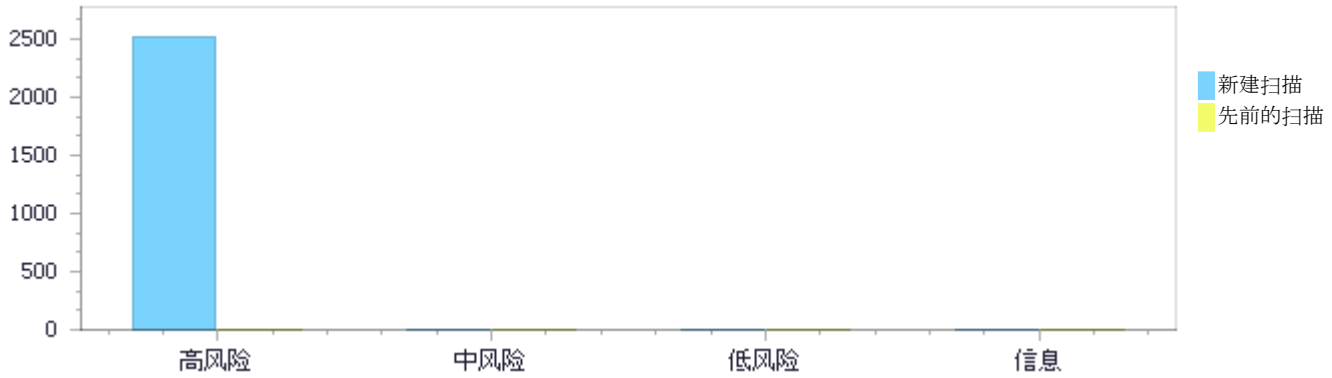
数量最多的前5类缺陷



按状态进行结果分配

项目的第一次扫描

	高风险	中风险	低风险	信息	总共
新问题	2,522	0	0	0	2,522
反复出现的问题	0	0	0	0	0
总共	2,522	0	0	0	2,522
已修复的问题	0	0	0	0	0



按状态进行结果分配

	高风险	中风险	低风险	信息	总共
等待确认	2,522	0	0	0	2,522
不可利用	0	0	0	0	0
已确认	0	0	0	0	0
紧急	0	0	0	0	0
总共	2,522	0	0	0	2,522

扫描结果汇总

缺陷类别	数量	严重程度：
SQL Injection	2341	高风险
Second Order SQL Injection	58	高风险
Side Channel Data Leakage	50	高风险
Reflected XSS All Clients	32	高风险
Stored XSS	27	高风险
Client DOM XSS	7	高风险
Malicious Program	7	高风险

10个最易受攻击的文件

高和中级漏洞

文件名	找到的问题
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	2058
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	979
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	978
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java	938
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java	938
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java	890
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java	890
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	501
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java	446
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java	446

已扫描的文件

文件名	文件大小 KB	检验和
/WebHallCMSV3.0BAProject/build.properties	5	4f8e1f91fc22f94de728fd0fd8e906f1
/WebHallCMSV3.0BAProject/build.xml	5	d2bfc0015e8fb2caf7ee59f0d4fa85a9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsAcquisitionAct.java	13	971b43b5d588ba08333f842311b5b027
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsAdvertisingAct.java	10	c94687ffc63dc9931038483b8e3494e6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsAdvertisingSpaceAct.java	5	cc91d80f32609c028f7071afe8589a23
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsCommentAct.java	5	d82b08c299426679daad7325d613ed52
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsFriendlinkAct.java	7	e5812fb6b0bf58123151704d9438cd89
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsFriendlinkCtgAct.java	5	a4548370a875e48b222725029c0d28fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsGuestbookAct.java	7	f54ff1f6efedeef7589a77d39e3de78e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsGuestbookCtgAct.java	5	161b6defbfbbefc8d43bf366c59e8384
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsKeywordAct.java	5	8f3362a0bd432a33a925c1134d5a32a6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsMessageAct.java	20	ab5a9960353ff2c1ea4ee34b01ef26f9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsOpinionRecordAct.java	2	89948b6867c893943e0f555f52f2543d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsOpinionTopicAct.java	11	a4ecd7ae10d2683f9fc4ef042720ea8b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsReferComplainAct.java	5	388d64f40b480503c301f028cd22d1bc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsSensitivityAct.java	4	658be40438fd9ba3d055be0a913c819c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/CmsVoteTopicAct.java	6	9d4c39b8b2d58c6f6d1d5bcaa28be434
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/ResourceAct.java	10	723732487594ad31a8d8e8fef4283b19
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	14	7b5385140e7c401fd13dc8fd04a3b967
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java	50	f339dd8649a347864cb09a154d298bb8

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/CmsLoginAct.java	10	69a2b51b57a0acbf259d81bb0e9aa099
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/FckAct.java	8	a623e6c048e51b6b440bf6b7e4062c09
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/FrameAct.java	3	0217a642bde3f6765cf49ea84c26ae7e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/ImageCutAct.java	5	e14c47c6bf6c705623fc7428dc54337b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/ImageUploadAct.java	8	22adde59bf56c095512e7aa587ce0b93
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/ChannelAct.java	14	1b6dc64df19cbec082248a9600af448f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	3	d657c37220c46519793332d9b5cb2d69
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminGlobalAct.java	9	8c8158c3f0ce2dbfdf7bf72fa5339b8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminLocalAct.java	9	0b57017b8dbb7af123e5c1fa3d4959f9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsConfigAct.java	5	d0b6067fb9b467fc7e5ca2ae4ee87fea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsGroupAct.java	5	2c4aea997a19c54dcbcd9d31e5eb3f0d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsLogAct.java	7	8dcd9a69b675be0dea345b72fee0d854
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java	7	74025c7691eb1853bd006c60b6c9406b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsModelAct.java	6	c39bf31574daf681dbba0776559df68a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsModelItemAct.java	8	78a760ea8dc9352cc30f4eab188f8e24
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsRoleAct.java	5	5346b42a7d02380042f4f91020d6e046
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java	6	6c8a39d2dc91c2246e83deb9e2bf7cd9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteConfigAct.java	2	b91f4a027bee9375d476554d503e10c5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsTopicAct.java	9	78e9141d11c546d55f17c5a76949f20d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/ContentAct.java	32	bd78c101c0e1a8875dad1c6b5e6891c6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/ContentTagAct.java	5	616bc2418140a2aa69c98adecb2e959a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/ContentTypeAct.java	5	68936ed913a7c4f87ae5ebffd0bdb70b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/FtpAct.java	4	0f935c7207a373e90451fd12068ac80f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java	5	7f5023883247eaf990a76ad63d7c1646
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/PersonalAct.java	3	43efe290b3e8d9712add5b3a4e73e7f3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/WelcomeAct.java	3	e31d725f43b9b12739d02e0193000acb

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/abs/AbstractChannelDirective.java	2	b3f705ff5502b88c5ced35923e61af99
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/abs/AbstractCmsCommentDirective.java	3	a60c1d018f4e37dd971806010c220f18
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/abs/AbstractCmsGuestbookDirective.java	2	51efd23e8e8a0595846f1b77123c9657
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/abs/AbstractContentDirective.java	13	47dcdc3b76fa2b034d369ca0d9b4b279
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/BusinessCouncilDirective.java	3	0ba97f0792f3e0e30e2aeacfc9549549
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/BusinessTagListDirective.java	4	f8598c1ccd1c582332515a641536f88d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/BusinessTagListDirective_106.java	6	a108118bb25f0cf78a147f35f1a8bbe8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/BusinessTotalListDirective.java	3	fdf78624aff2bad163ee8fc1e02e280d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ChannelDirective.java	3	7a4e968109733d4d0140dfe7e4d75e52
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ChannelListDirective.java	4	8afdb8aafe508a96b21368f44002eb8a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ChannelPageDirective.java	4	f810807d0f208a4201499121123379db
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsAdvertisingDirective.java	2	7b37c4a2e4ebfc7a1d1026f4a6b1b21c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsCommentListDirective.java	4	491f4e4d24b680cd388e1ea0181d4773
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsCommentPageDirective.java	4	bfaaa0b1fb39e1c254b383051a4fe501
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsFriendlinkCtgListDirective.java	3	3a01aff3d2e781d0056778b3e4f041f9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsFriendlinkListDirective.java	3	27cc886e9eddb56804c7451f9edae181
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsGuestbookCtgListDirective.java	4	1b9fb88cc1c71b476b6e0c9ad0ff4e51
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsGuestbookListDirective.java	3	909ae602d4d8af65c9be75f99b2d377d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsGuestbookPageDirective.java	4	85621a2e2b62905d114819299245f7d5
/WebHallCMSV3.0BAProject/src/com/jeecms/c	4	672c2a4d365cae95ef96242e5eea734

ms/action/directive/CmsMessageCount.java		c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsMessageCountgr.java	3	fa435e621051c317a3cf4ff701ae566b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsMessageListDirective.java	4	da15fa18b288ae6ce82be542c948cdfe
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsMessageListDirectivegr.java	4	f401d2b300d721fd65a660ead36625ab
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsTopicListDirective.java	4	0a7c0fb12b894268ffc40544a70a5753
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsTopicPageDirective.java	4	6d6f2c7f1971663d48cebe12dda00cdf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CmsVoteDirective.java	3	580e2cf729968d903d76f5674a452821
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ContentDirective.java	3	5ef5c42abc257587db94f8420f33bdde
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ContentListDirective.java	4	41590a7c2eae20f8f97ccdbdaec679ae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ContentPageDirective.java	4	2bfa3ebcb3189989e43c66d4ed4326c2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ContentTagListDirective.java	3	28d264ff06eb2693d7104cff20d531dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ContentTagPageDirective.java	4	1e4f0895f0cbe4468f0adbfd76519ea7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CoopBusinessTotalListDirective.java	3	4a9bde1b5adad94c53e8dbfd7287993d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/CooperateBusinessTagListDirective.java	3	d96d11813a11e238169cf2a61c2716f6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/DeptWindowListDirective.java	3	3227f1489d1cc1230f3f995e446eef4c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingDeptPermDirective.java	4	28701c39ddfb93a6a4155981e610d28e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingDeptPermDirectivegr.java	4	8fdcace42160e1973eb671a863e02f41
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingDirective.java	4	c2fd11e45b5b2d5ea334151914e67921
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingDirectivegr.java	4	c86933e1b129cb0414468021cc83241b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingPermDirective.java	4	889f82a409914498af2728552e7d56af
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseBanShiTingPermDirectivegr.java	4	42cd29cb62f4f9ea574b1600d0972892

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseGuanZhuLanDirective.java	1	21d60dbcda86dd665293935398dd76bf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseUserCmsFriendlinkListDirective.java	4	7aba7a72b1d716592e0658b32bc704a3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/EnterpriseUserCmsFriendlinkListDirectivegr.java	4	6bf90ccb86a433ae823e6e56ea78d5c6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/OpinionRecordTJDirective.java	4	7ddbb79ce80c7fa5d39846c7898e4db8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/OpinionTopicDirective.java	3	a4feb59858b0564f6304cd4cb6b22c00
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PaginationDirective.java	3	016411275563a568123c7ff5a4fdcf5f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PermissionitemBySxbhDirective.java	4	fb2abb3d953011ea9228d17435f0bd7c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PermissionitemBySxbhSortDirective.java	4	6a8e6915e62a1c76edecf730536d0f8b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PermissionitemListDirective.java	3	c18389eaddd4b984a1bdda0083f61e5f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PermissionitemsortListDirective.java	4	2d56c2c3963d646457a6c30b2964bb1c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/PermissionitemTypeDirective.java	4	680cb3dab631abe1971d25692a289f10
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ReferComplainListDirective.java	3	bc465d3be60c0c1d37670c5d4cedcd0d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/ReferComplainListTJDirective.java	4	85df5ac284ad4bfb6ca358e993878462
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/SurveyOnlineTagListDirective.java	3	3848d33a808ed0ed642c69fa097e7c90
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/SysDeptListDirective.java	3	5c23be2c9fe8857386d56fbb8e38a104
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/SysDeptListDirective1.java	3	bc1773744550ea17679407ff490a0403
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/SysQzqdDeptType.java	3	a39c43537a045b6bcd6ebd847d05a49f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/SysRegionListDirective.java	4	5c9357a4911f3436b8559c8229ae3d6a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/TFlowNodeStatusListDirective.java	3	527f67937ba2eca717ce2d2fb74e0d65
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/TInsAdviceDirective.java	3	0e8defc2bef2a4373a051d02ec0929da

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/TWebhallGrsbClxxCount.java	4	4d6c8eb87328c037d8c1ee991bc75b6d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/TWebhallGrsbClxxCountgr.java	3	16cf023ad3dbb62b9cf01cb94db711e8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/VTInsAdviceTJDirective.java	3	e18526033f382e1388a90a3f5146b058
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/VTInsWebhallBusinessCount.java	3	dbdc23d19f3931270de5cbdb03a15ec8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/VTInsWebhallBusinessCountgr.java	3	a0f44964352e95e487af6205e3eef7fb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/VTInsWebhallBusinessTJDirective.java	4	39f888b3a739b23205d3a203da6871bc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageFavoriteCount.java	3	599a616e45c12d55606fc85a2fe32e52
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageFavoriteCountgr.java	3	d3b0e9634703f45dd43a318b1ad042f4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageFavoriteList.java	4	39fd8183d29e22a6551d99988221a6fb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageFavoriteListgr.java	4	c6f4ceddb79e0ce94b9910b6b17d4cd4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageReminderCount.java	3	c5ecfb8b80b19f542027e4cf32998058
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageReminderCountgr.java	3	9d73800ed3fe1ac1e08b23cf985b55fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageReminderList.java	4	272da9283d6453218d3c456419cfd9db
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/directive/WebpageReminderListgr.java	4	bdb2c3aba315fa0e231bf1cd00ee1e4b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	3	e76ad7d30b0702d0732015e185c998cb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AttachmentAct.java	4	9cf5c0e6c51484fe55576ca904b64c16
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CalculatorAct.java	2	03d8639814e120121af4cccd980d0610
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CmsSiteFlowAct.java	2	b8cf3632714f7e195e94e4df979efeb6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	7	312ca0fae0edb25f546551b2bdaf9196
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	2	6ec8c23df821003eb905c65d6d6442ee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContentCountAct.java	2	43822c2e5577f209087519e93b446e08

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	2	b633937c1a1fff79b24d3e6aeeea2caa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	30	d05723ae08020b5dda30b81d5c3bb78e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	4	4f76bd74e946bfbcae2f1803f00b519d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	5	aa1659da2f5628ffcb45be2a00e989e8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	14	238c53154b3ce9798d2e1fa7780c5d9f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	6	0a550d8c81a140aed7bd070aabeddd91
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	60	3fd80abe0219efd83c11ea37e76a6c09
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	10	44a299dc7ad5e7fed9d5ddf8302d3b95
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	8	cc711778858ea7b9a517e90a9f54a09a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RestTestService.java	2	fdadd1e7281900f8ede7c831a1b4870e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	1	b101b810876db110ab16abda02175f2c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	2	030ef374757389816a88219cb8b743e9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	5	5934135723e3d07bdc28049420734171
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	3	fb5bc070a7d9f090b3a95ca94ebdc7e4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	2	6b082f6170ad09948318a4894474693b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	4	b7e516e5a0727f387286317581d75950
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	4	4878a0bcc82ed2723a25d552409ba84e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	11	e92e90f2103617f8ac711a3333a8b2ea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	5	96a6514024b9c3c9f2c3201c46847da9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	38	571d329d5ef34dec62e83bf5b668b3b8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	5	38012f8b76e84e27831df8c6f6b48211
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	21	44e0c60820fda691259d88014a42f8d8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	12	1a3f52adffc606067628cbe741d99151
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	29	14bec958004c8f5a056506b7af533bea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	4	4c5f08cd2be87885431bfa230a5979f8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	7	bf51405a71ddde056892c65aa890fffc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	14	428bec4405fffafb1c927fc5d5f3c535
/WebHallCMSV3.0BAProject/src/com/jeecms/c	34	c0dad93c1376c222439258f869321a8

ms/action/member/EnterpriseAct.java		a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	33	b67837057603087dc5ec5285d520684d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	48	c000ef9cf23ea1e1fc72dad108e2eaf7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	41	1823f9146f8ebb8e3667d1c5cf510a6f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	23	2f7009e5e0bb54710d1a1b262d6cab2f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	23	5107447d63f91a904b4aae645271bd46
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	6	500dd52028b4f385dc97bc8edea784ce
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	6	98131e44a8aead2c4e8919a82cdb0701
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	9	cbb382e1887763ac6786fd8dc7d3ff3e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	9	99645cfb264292ed7e63034317b4b6e5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	8	9c033bce338a4853d85f2c03ce9ea318
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	8	4ce4a4549b4d41dc738c139762c15c8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	3	753961dce69d7968796eb2dfd0c7b46f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	3	04db075be570d7c49444d1ad3f5a6c23
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	3	ee700726d97f83b52de910fcdd76ee42
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	3	b715d8009db839f2089e7dc174d91908
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	11	467581ea296e878dbde5fae91d784b75
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	11	93ab8564eb329a1d2633ce60e2bb7eb5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/FckAct.java	9	ac65b68d3265466f9a1a7e36c498b824
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	7	3380d58e1da5b65fe8ae2f8715c0e73c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	5	a1c0445a97cd416653e9002a8bbec4b3

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	6	bac756a6dddb034a742ef4e8b8b5bbe6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	9	8c643b02cdff3021969f0304c81faf72
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	1	7aaec5ceee6239126b489ed90e03d038
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	16	dd3c39ca7aaaaea172bb59296a08e66f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	27	a2333bfbd4d1c997f0047776b2fd396a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageTask.java	1	6a25c4f04283879489d67046afa61ada
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	5	00d681981c40262b7dae6fc643d3443b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	14	7e37144859f4d37011d25edaf334ce65
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	14	430756e87ecb5ac5ffdca668cb29ce1f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	30	8652ce1b639c79aa546b18cdda8770c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	9	34c50bcccbeaff60dd7e58fc58be50bb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	11	a79c15470d33db3741eb2361cd163830
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/Service.properties	2	729f29e3c652a380e68a1f4dada77ae4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	41	0e2fb2a259a5eff66a26254dec29e68f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	17	470d2dbaa5cd55e23682b25af7d46183
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	41	6569fc42411a65296ecef2348f1fe16d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	4	6520064df4d59a8f6511e157d5c3378c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	4	9f05087b5d9fc7a6355a4d74f51ac37e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	13	2ff082d52bcca5f748e4e5d3c6c9021f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	3	817935087d57e8effd58bb7a15419ce7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	2	183d3f108a9e807ded1643f7e80f6966
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	17	e2fcd59e2453dabfcb026204ace13100
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	13	3f82ac8fc2bebb6f9aee1a374b41f657
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	4	c1cd3525d6751e978e8aee219532e51e
/WebHallCMSV3.0BAProject/src/com/jeecms/c	4	07bfab239c5339c1b731485c8cf7427

ms/action/member/WebpageReminderActgr.java		a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/AesCrypto.java	4	849d3afceb377acb6f93be767617ac51
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/BASE64Helper.java	8	1834edad2e361e7af0fd4422ef4eefa4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java	4	979638a8018051aaed2f78cc6c8589fd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/CDBManager.java	6	1d41e591b278db9641af05085af0d341
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/CheckCodeServlet.java	4	0c5c1392166c9cb411292461deb5c531
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/ClFormatXml.java	7	232f14dd9000134bb24d75b7eb2d58d1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Constants.java	4	75534e693ef8a1d262bd0c3f6da4f878
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Content.java	2	14fb2553d644017eee7d7c76122674bd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java	22	9d170f2b47efaaa5a0ee400a48896878
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsAcquisitionDao.java	1	67d7ccec43d72c2c96448a68b844856a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsAcquisitionHistoryDao.java	1	156c26b3558d82cef0e93fafb970e790
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsAcquisitionTempDao.java	1	02596bf500d2db5cfb622f5f07d392fc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsAdvertisingDao.java	1	ddbddb7da056b53a6a41a4487d92e9f3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsAdvertisingSpaceDao.java	1	4a3382606f9b6c73c994d14b869f6d6c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsCommentDao.java	2	3495c85ac332e3744f8581b63d7d959d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsCommentExtDao.java	1	b863acae4ec836feefd737a0d064b9e0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsFriendlinkCtgDao.java	1	9ab551c451424f34f3e3923050d373c8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsFriendlinkDao.java	2	c1fa13606e7db9e25e8d8faa6db4aa05
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsGuestbookCtgDao.java	1	4de8d8cfcd470777cf093bd1e6d29835
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsGuestbookDao.java	1	ff69ea60f2f76c0de87ec7bffd45d217
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsGuestbookExtDao.java	1	ee682f912e7a600dd9de06681af48d7e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsKeywordDao.java	1	491624e127e3c17241c13901cb760d88
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsMessageDao.java	1	0e1074d39d114f9c1599e920a988a5ba
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsReceiverMessageDao.java	2	eac0ce00b2d28fe42e13600bea2b04fe
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsSensitivityDao.java	1	47f80927bc1f4c195d1c3bcce67210e1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsSiteFlowDao.java	1	7d92beae30ed9ded42bd8b6bcd79c858
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	9ee8ba1078084dade5232209b93abf

ms/dao/assist/CmsVoteItemDao.java		17
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsVoteRecordDao.java	1	9e3cd37dce022a8758d9419c592254a5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/CmsVoteTopicDao.java	1	954394908dd2bad698165e949a370e72
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsAcquisitionDaoImpl.java	3	c6fe5ef1f4efdd9b4811f3259d33bd94
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsAcquisitionHistoryDaoImpl.java	3	5784da8c8b73830b0e7554b009993bdc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsAcquisitionTempDaoImpl.java	3	6af19aa3127f4b59c001c2fe77810ba8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsAdvertisingDaoImpl.java	2	303d91b50d06c1875c631222d2bfed7c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsAdvertisingSpaceDaoImpl.java	2	90ae71cb4438d8ffb74e604f8c3b5dac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsCommentDaoImpl.java	4	5b0b18b32dd3bdeaf381a4e5713bb603
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsCommentExtDaoImpl.java	2	44b0174cf2b10675ea9d636c59b638b9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsFriendlinkCtgDaoImpl.java	2	cf285179c2daa4b68d986ca04983a6f8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsFriendlinkDaoImpl.java	5	205dce5465217aa9fd66d8efe357293d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsGuestbookCtgDaoImpl.java	2	06a965e7c41ef22a88832609052e689a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsGuestbookDaoImpl.java	3	ce6aaa01c13c2ac0abb95f9da356dcef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsGuestbookExtDaoImpl.java	1	22832e8f31248bb878511c9c58a3c446
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsKeywordDaoImpl.java	2	c54050cb224f9c1ab1ec25d457c0de18
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsMessageDaoImpl.java	3	4fce621375fe583a52bbe59133f0df92
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsReceiverMessageDaoImpl.java	6	fc86415f70615fca68e367797cdb0032
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsSensitivityDaoImpl.java	2	47dc6761f793463e3a03c7a3d815f28f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsSiteFlowDaoImpl.java	2	abdf5c752505401adb70b335bd36eb52
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsVoteItemDaoImpl.java	2	40bc9acf0c711cbc0e208f33fd19c774

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsVoteRecordDaoImpl.java	3	4b94c764f84a79179f4621ed9a173621
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/CmsVoteTopicDaoImpl.java	2	e996a6480a25f24a61f3d747df10e2b2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/impl/TYWLSHLogDaoImpl.java	1	daf16d5f3ccf0e6f370542f78ba72f76
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/assist/TYWLSHLogDao.java	1	b8b4cebc22fb17f65c0556e213572f09
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/BaseDao.java	6	48dcb3483cf0f99816b0d66f72421d96
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/BusinessCouncilDao.java	1	e01dad59430927e0634ff33dcbd31050
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/BusinessTagDao.java	1	639ebc662d4ca848b8bd53edf8d737b6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/BusinessTotalDao.java	1	4469b1db112c8915582b3ad85df39a98
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CertificateinsDao.java	1	2afcf4e68d02c612aab1fb7e885162cb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ChannelDao.java	2	347186c8b493a49ca8856aeb9008ee87
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ChannelExtDao.java	1	6e1250a913f63bf38fbffb2183771ac2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ChannelTxtDao.java	1	1c0bad8e8a6462f6c659c284fdee0a99
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsConfigDao.java	1	63152b8395478e9d3ebfaaf848df3d1d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsGroupDao.java	1	fdf70ba65bf019b44e80d9df3db5acb4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsLogDao.java	1	b59ba3dc43ae7310fb4d39b6503767a6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsModelDao.java	1	1d7ea067b3fb48632ad4302365ba3891
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsModelItemDao.java	1	f42ff52d150e8c0dcb4a7d36bea86610
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsRoleDao.java	1	e63ee2f65ca1af28f8accb6f2c560309
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsSiteDao.java	1	2813f4fe01ec0a6fa92c83bcd87f090f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsSysDeptDao.java	1	3ca43466ecb056e5b3623643116b3fa3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsSysRegionDao.java	1	c570a70bf2f34e94717bff25b1964c91
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsTopicDao.java	1	b539ae86892938aba2f21dfec87662fb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsUserDao.java	2	fe6a1bf0e325cef631b3277e45ccf912
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsUserExtDao.java	1	3d9d3babcd60a6bede802576d5f0d352
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CmsUserSiteDao.java	1	09c1d76a85b89014e78a6d3968e8dccf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentCheckDao.java	1	1e77ed4940ddafbff54d0b6af6ed5ba2
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	a6f81ec6d2fda25f461238f91742a48a

ms/dao/main/ContentCountDao.java		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentDao.java	8	550cb0062b5fc0fe6e62ef51112ef82a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentExtDao.java	1	85f158ced1c11ec1a1f1352bb995c391
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentTagDao.java	1	86cf6e5d33caf6b44162434346caedd7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentTxtDao.java	1	f87aa3d589af877404df082c6098b100
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ContentTypeDao.java	1	6df03d86a37bc13a1d263049fabbe2fd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/CooperateBusinessDao.java	1	b4be554cb78764f659c863ec3a17cdb3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/DeptWindowDao.java	1	2da6833e6141c3fb95605b3364412f85
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseBanShiTingDao.java	3	f5382e27c33c50490d063cb1c24c8a4f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseBanShiTingDaogr.java	3	567a2b959281bec91f483586cfa31b37
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseGuanZhuLanDao.java	3	d4b2507ede8fd79a53ed3d35669ed2c5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseGuanZhuLanDaogr.java	3	71ca4058533914c1247016e60716388b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseKongJianDao.java	1	0a0290ee203b7993d8f6a57b19c75339
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseKongJianDaogr.java	1	b6dea858c130b2116ff3cf867b8a551d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZhengQiHuDongDao.java	1	5b9fd08b0cedf5a7cb86ee2295440150
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZhengQiHuDongDaogr.java	1	5bc65b010c7b6ab9b0dd1ce8aee7b565
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZhiTongCheDao.java	1	1378aebea6079b3c401fd7f5033f9727
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZhiTongCheDaogr.java	1	63035194d388cd2183c00a39c2e25e72
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZiLiaoDao.java	1	424142d82002a2b2e4288e2a7dd76859
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/EnterpriseZiLiaoDaogr.java	1	65232af4f6e1ff9401955cefb1e385da
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java	9	2e71249a618e402795d3d6eedf23e2a7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessCouncilDaoImpl.java	2	cf68609c1c1e80cd0d7a312144f0422b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTagDaoImpl.java	5	aa0a38e70bffd442e8e1b0f56b73fbd9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTotalDaoImpl.java	1	45a9e3ad7206b6305acd100067aa2611
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CertificateinsDaoImpl.java	1	8b46763a5b8fa4cf2a000a67c7b5c902
/WebHallCMSV3.0BAProject/src/com/jeecms/c	5	0ba9ab4f1ce8dad9ec502c966c13446

ms/dao/main/impl/ChannelDaoImpl.java		0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ChannelExtDaoImpl.java	1	d67258913f35de89311d59d45af7c606
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ChannelTxtDaoImpl.java	1	0b845f77876b97c8595b0ee9f1aa6059
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsConfigDaoImpl.java	1	a23723c88411d0753994b464d59d3ed9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsGroupDaoImpl.java	2	f411c69b7c177514876fa915af3d30af
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsLogDaoImpl.java	3	97fca7bb4d31228097e26d4c6f4227ef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsModelDaoImpl.java	2	28f88434d6a9600d9ef678ac568f9ab4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsModelItemDaoImpl.java	2	ebcf4c1847031faf3c69dce03cb8fc74
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsRoleDaoImpl.java	1	7b059b119cc913752218c443ce4053ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java	2	6a2e9f058fef872057af3c170e6c62f9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java	2	0690e296e6d7c9e0c321493c855c5361
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	3	ebc6d00d01219f77323344ff4a5a484a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsTopicDaoImpl.java	4	9e0b23547c02a2b599812867974fda81
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java	7	8f46c0ce7f1b70538dccf237c848cf6e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserExtDaoImpl.java	1	2e74b2c19bc42e4b168beeae0557bcc9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserSiteDaoImpl.java	2	427df2f8d7030b4eba9d1b0a4bbdcb59
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentCheckDaoImpl.java	1	a6dfa720bd8ecbfe5843668db4f75892
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentCountDaoImpl.java	3	ec30bead5d902ed820acb8fcada56b1b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentDaoImpl.java	25	74a733d489aa070016d5f1cca4e0902b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentExtDaoImpl.java	1	421ee2e169524d0ce3adb035359259b3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentTagDaoImpl.java	3	3b0a096ecc4f0040bbbc1e1e8dc1635e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentTxtDaoImpl.java	1	2fa6048035a5bcf7b388644d0264f4d4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ContentTypeDaoImpl.java	2	d71abf30c30ea17816db17f93bf70b46
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CooperateBusinessDaoImpl.java	3	40208163d13ed4fc1028aacfa64c4b9e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java	4	60960b82c0ad4bd5963c81f9eaf66e56
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java	13	f6f579f78cafe3161da1449b21b4f7fe

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java	12	07028c94faca81af41b96646d73a955f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java	19	ab788018da7379072d485c47a4d4ba00
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java	20	e1c61a4615f4bb3967b4c70781002e71
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseKongJianDaoImpl.java	2	eaa4265b2aeb8b0eaead02b0c0f25321
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseKongJianDaoImplgr.java	2	22661931b80d19ddffde01902699df7b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZhengQiHuDongDaoImpl.java	1	7c76bbba478113506e4364dfa3f307f0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZhengQiHuDongDaoImplgr.java	1	82d6f98c832c51d5abc61aa6e7b4b524
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZhiTongCheDaoImpl.java	1	44f54be083cd568bb263935934c62d48
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZhiTongCheDaoImplgr.java	1	5dad21f2290d9dc4b47dc93c157b93ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZiLiaoDaoImpl.java	2	ad5096410da3470de277a20a102b76d5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseZiLiaoDaoImplgr.java	2	491d26a3e201a71d57d5c012716792dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java	19	87fa47d0eb96247167f6b47eab15dc0a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	38	867ec560078e694634147e6286ad1e17
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java	13	6ccbbb48db7df8642aea9bd93bf10ae4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReferComplainDaoImpl.java	4	0254eb215e611fe42fdb2da4cf3cc7f3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/RegistrationBureauDaoImpl.java	1	c16b7bf97d220a4368f7658c19a7dfbb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java	2	a5156d789364f5ec6a6d9498164fda2b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceAttachBaseDaoImpl.java	5	3349c995396ee3dd12eca57fec0abd80
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceCertInfoDaoImpl.java	6	c0970289478df408b114df1d44080362
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceCertInfoExtDaoImpl.java	2	51f11576354601e138320e07eb658b8e

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceClxxInfoDaoImpl.java	9	5a3c4b707150f817214bd7b8c6cf62be
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceDataExtendDaoImpl.java	3	1aed1753f22c6778d79bbe7d27851b8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceDataExtendValueDaoImpl.java	3	7b693a208b7d678c1b019bb685c3ebcc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SurveyOnlineTagDaoImpl.java	2	6fead6b931379fe0ddcea19290442bef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	2	e2594123922cdf2ae49fab8eca08d363
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TFormLibDaoImpl.java	2	22b1042aa29316bdb99bb5f315575d36
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java	4	a8099165e48c27059a787bf15558c09c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java	2	9b7be7190955b4f18d472b7aae0ff741
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsFormDataDaoImpl.java	2	dcb016cf84d4b1001fab77e57d47d1b5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsMaterialCompareDaoImpl.java	2	f44cfe51b09b97cac41b3780721d0171
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsMaterialInfoDaoImpl.java	2	c6d8fa96f61bd6756b765d5f6a35f7aa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsMaterialValidDaoImpl.java	8	815b65da511ceab6e1c2c2c5741dd101
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsWebhallBusinessInfoDaoImpl.java	5	8470dc527f9fb98fe6efe9bcd3a70b4e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TOpinionRecordDaoImpl.java	3	2d6dd98496cd30752ce45e4169d53aa2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TOpinionTopicDaoImpl.java	4	2a451310916a671d3a797847b472ef8d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TQzqdDaoImpl.java	3	f5101ef1d81082f50536fdafaa136054
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TShareClxxDaoImpl.java	7	f7f6cb6233bd6c336379ba1b47bbc391
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TShareFileDaoImpl.java	3	7bba34a71386d7f5965933e0f7e45101
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TSpsxPermissionmapsortDAOImp.java	3	5875cc30308edf32af7c3ac20ba51140
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TSpsxPermissionsortDAOImp.java	2	b96d67955247b0f5f6ef2a82e1ce8aad
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TSysFlowlibmapformDaoImpl.java	1	924c70f691f7e98c5fabbc71bab6a36c

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImpl.java	4	1c1a0d332cdc29466d6bbb1b2216c05a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImplgr.java	4	282209c667e2b32eaa40a111d54e9394
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	2	bf717abd8dec32680c17dd51f7f49d31
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/VTInsAdviceTJDaoImpl.java	1	31a58094431ef67124614285ca00bf43
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/VTInsWebhallBusinessTJDaoImpl.java	2	2ebe66969ffb2bf040fddacffadfb739
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/VTOpinionRecordDaoImpl.java	2	abe89c6452ab968b4bf874a19fd783f7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/VTOpinionTopicDaoImpl.java	1	f4d9381e6a8bd4860ff96a7e5160ffa6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/VXnjcDaoImpl.java	7	6babbc29d32a80f5f7ef5a463804bc74
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinessDaoImpl.java	8	54935218e86bdddd7306d9ece00e54a7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebHallIncInforMationDaoImpl.java	2	a329165208d1a34eb9d37dbfddaa2bd7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebHallUserInforMationDaoImpl.java	1	5dcac74c551f15f24856cd6428f65d51
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageEnterpriseDaoImpl.java	1	f6cd87933ace9195fe6cc7a164e75487
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java	5	4254e52fa6ec472a2c327f91ee5ce3fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java	5	422a46aac3db2564932d7c9f90c2c2a9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImpl.java	3	af49df322937de2d10554246321b3ff1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImplgr.java	3	fcdcaa031fc9248c92f377c6046fd02e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	6	38d3c306cf156aa56e4bd48265c41ca7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/LawGuideDao.java	3	25a09ff7e435bab51c7febb8ab1260de
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/MatterDao.java	1	9ca0b484d4d7b3ad76b812c7fe83d44e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/PermissionDao.java	2	852f26e1564726a244ce556b2cb9149d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ReferComplainDao.java	1	8ecbac28f25959a963d6fb77ef5a5c1f

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/RegistrationBureauDao.java	1	312248e3cfdfaade853ed5a5cf0aa426
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/ReservationDao.java	1	ed4b66df9afb5d754899a144eabc0b64
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceAttachBaseDao.java	1	e8a6004a996d408095e7f47a1af28737
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceCertInfoDao.java	1	b16a2aea695c897beafe8c64d34cea89
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceCertInfoExtDao.java	1	4932c54a571494a4bfb356645490db5f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceClxxInfoDao.java	2	eb8e7c6ea01504a00d9436916a66c701
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceDataExtendDao.java	1	5068522849396e0b27cd394a1b8340ba
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SpaceDataExtendValueDao.java	1	5f1821174eb8c763a2ac96743d086972
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SurveyOnlineTagDao.java	1	5175be36321c675e2f59405f5151fc9e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/SyncConfigDao.java	1	0db71954f88f3ba5c0c8ab9bff1ae433
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TFormLibDao.java	1	ffabc4f71f9c043f514b65e77030886a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/THrUserDao.java	1	7d747d65486bdd2e9a22815159606c9d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsAdviceDao.java	1	4a1fdf8afd86a98aec41d68040845de4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsFormDataDao.java	1	9665436541c32c450436a89740362f3d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsMaterialCompareDao.java	1	09e69dfca8c7c6169ec837b6a14a5901
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsMaterialInfoDao.java	1	7c07efadf2612e7bf6813a07340c35cc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsMaterialValidDao.java	1	a0fa04bc2f35d28eaf1ed571209772be
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TInsWebhallBusinessInfoDao.java	1	85e6823bc2ff4ddd80ab94a80eb82881
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TOpinionRecordDao.java	1	0f9f13f087da91bdde0b7184313d0723
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TOpinionTopicDao.java	1	acce5e0df8af0bf4eb163a2b1a83b5ef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TQzqdDAO.java	1	98af40ebc7f45d4bda9da830b9bdf5dc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TShareClxxDao.java	1	7e66d04320e8b35f1327591b73a69cc0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TShareFileDao.java	1	68e032460c91c817e0fcddb2ff6a5f12
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TSpsxPermissionmapsortDAO.java	1	c4d46fafb5a79feb67b8f7f901ac2b01
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TSpsxPermissionsortDAO.java	1	d2fadcf20751c1405788be4b0bc4abbc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TSysFlowlibmapformDao.java	1	cb4bd26db994c5e373044761e27abc1a
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	8c849edff7ba9e760260ff2db8e6387c

ms/dao/main/TWebhallGrsbClxxDao.java		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TWebhallGrsbClxxDaogr.java	1	4353bcef20cd944c3ef0fc2f52087e31
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/TWebhallPostDAO.java	1	49e87d9d9a155a3f86923022e1502115
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/VTInsAdviceTJDao.java	1	ba74b2177466489bd3dce765933cac13
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/VTInsWebhallBusinessTJDao.java	1	d7790a7fb36a505de9d2bed3577e6f38
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/VTOpinionRecordDao.java	1	24ea22394534aa5d2c6edadea41b3582
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/VTOpinionTopicDao.java	1	54d9333340a80c50f7f29f78317eb282
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/VXnjcDao.java	1	cf12f21745e9192d87dcb2eca16cc4b2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebhallBusinessDao.java	2	ede26eba2891642c2646bba32292126c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebHallIncInforMationDao.java	1	1c2186d027596a35d21ca9b236d33bbc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebHallUserInforMationDao.java	1	c206a772b3c61c4a0f8d50f5f34f0b30
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebpageEnterpriseDao.java	1	53f5c3762b436c4ca1424d7612af277d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebpageFavoriteDao.java	2	9a3ac346bb3e226d80cd3e82f11c7aa8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebpageFavoriteDaogr.java	2	583f5483bd48cdae453d14369de401b7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebpageReminderDao.java	1	33e162e4a3d172f253172551df54cd23
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WebpageReminderDaogr.java	1	dea5033c18668d6017b996a05f6c14bd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/WssbDAO.java	2	c240f2df937a5c8597c92e110e09100e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/DateTimeUtils.java	16	1237b8b212cfa1c4edf6b6ea0ff2333e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsAcquisition.java	17	19d4f04d434bc48888df33183f03ec6a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsAcquisitionHistory.java	5	05b8dc626c68db1521bab54b52582356
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsAcquisitionTemp.java	6	5e952d7468fd94c6258f05e2539dcb84
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsAdvertising.java	8	e983444ed0b604abdcdf096188ec7d6e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsAdvertisingSpace.java	4	95ed11f21d58ed43e0d9ad426e6673ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsComment.java	8	ab809b963a63e631ee2af17b02524857
/WebHallCMSV3.0BAProject/src/com/jeecms/c	4	ab177dcfee0da777121c9b777369e96

ms/entity/assist/base/BaseCmsCommentExt.java		f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsFriendlink.java	7	5f56b64406d1e31b4956006cbacd2fee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsFriendlinkCtg.java	4	9ba2aa3e014cbb20c4d3700e325de2dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsGuestbook.java	7	d7e129c15be0cf68a69a3f0792e1db79
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsGuestbookCtg.java	4	e83f03a75076f00108fdf271a1c9627a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsGuestbookExt.java	5	15ba04b8717e2cc39f84460caae59aff
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsKeyword.java	4	2bbd5c949d1bb1c79106c14a4c371301
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsMessage.java	7	6743f231fbee30cc6c55ed1d2602ae1a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsReceiverMessage.java	7	e575260e760c446b69b88aed9233557c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsSensitivity.java	4	15fe10e31c94aa7893a1de4a988da8af
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsSiteFlow.java	7	5b49b9a1fe3048b659bcd305bc6b66c6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsVoteItem.java	4	016cd479b0cd0bace53c73d252b83279
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsVoteRecord.java	5	9e2cee1f90d762f650fbe036a249b091
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/base/BaseCmsVoteTopic.java	9	13c3230fc802f41abfb804e1d5a95c19
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsAcquisition.java	4	bbb8da8edb2a5f3504beed0741f5bb51
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsAcquisitionHistory.java	1	00116718446cacfc7073a575478b9686
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsAcquisitionTemp.java	1	cc7768d2a538d0d28e23ea7b7da9cad5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsAdvertising.java	2	5b6b6c38fa8e7b8099eb170db0892d70
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsAdvertisingSpace.java	1	e629b9e8dd73c8c003d657eb0908b498
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsComment.java	2	4c7df92478ad6674f769a3e3fc91bb25
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsCommentExt.java	1	b6536589ec852a8126b4d3871b09a212
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsFriendlink.java	2	3534616a89fe5ebf3a3397ba95526cff
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsFriendlinkCtg.java	1	5da193449067945572199eda12a9e0ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsGuestbook.java	3	71fce892c59061e6b6b8beee97922615

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsGuestbookCtg.java	1	4dd9a53c9171816a1ee08c28b8d30b20
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsGuestbookExt.java	1	b4d44669519d120db1f228eb499106e3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsKeyword.java	1	e435b38e2f6192e720cc49b3116f9a4c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsMessage.java	2	0193d78c3142d0734bf77906bf01455c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsReceiverMessage.java	2	7e47a127ebc8fe6a1b6a02b58b4c7131
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsSensitivity.java	1	976ef654dbb55a448d04dd706dacf190
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsSiteFlow.java	1	4cfccfc4152e266d67c91d00451b90df
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsVoteItem.java	2	68825eb4066941bebdb8c94cd70b67ea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsVoteRecord.java	1	2c043ad7453395a5302d823467cee94b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/CmsVoteTopic.java	2	a5c3775c924485ba53212f818d5c33f6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisition.hbm.xml	4	07a5e3c23419a4a2e1c87d5d306aad9a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisitionHistory.hbm.xml	1	0da9d1db0700aa1a198d588735066e67
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisitionTemp.hbm.xml	2	2978ec00c26bfa28139fa19ceaefe613
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsAdvertising.hbm.xml	2	e3584b9e58472f5a7e89879ff2ce865c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsAdvertisingSpace.hbm.xml	1	ec3743970cf9703c13c29274e94e3e7e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsComment.hbm.xml	2	d973053ed2b25bd98059ac9a559d7244
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsFriendlink.hbm.xml	2	cba76d4ee7fba07d9e711d60ba1d94c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsFriendlinkCtg.hbm.xml	1	9bb5af460f6862fbbc863d7df4d84402
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbook.hbm.xml	2	27b1010d765e930656f8e02df8edd6ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbookCtg.hbm.xml	1	91c737657cc3c0e9b5755a4f52fc3dae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbookExt.	2	1997712ce98b1325ae08fd0c8c1b9a2e

hbm.xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsKeyword.hbm.xml	1	4f17d895cfc2019616fe9b298e518408
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsMessage.hbm.xml	2	18af079d549e1025c224258256d999d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsReceiverMessage.hbm.xml	2	12063a668e2a3002525b64b0bedea9ae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsSensitivity.hbm.xml	1	45f7f7f8cc500f1d60535bcd26a0b241
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsSiteFlow.hbm.xml	2	09b3ba5c720b6073b213298cf26d939e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteItem.hbm.xml	1	a5d8598ed2b4823c8e6d69ee2236caa0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteRecord.hbm.xml	1	f6ee83f7726df69e9d0fc3a7120533e2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteTopic.hbm.xml	2	5b973992faae627b6e008e62177b691a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisition.hbm.xml	4	a56b8649837fa97492d36ef401053bc1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisitionHistory.hbm.xml	1	33b4da3bc005c0840dbeea7ce57a12b3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisitionTemp.hbm.xml	2	fba2e6072bf6e453b7da705b34bf9527
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsAdvertising.hbm.xml	2	c6511bc0babedb718d56a35d00161920
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsAdvertisingSpace.hbm.xml	1	16a7c9a9aa0a4d08379e384fc0fe94b8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsComment.hbm.xml	2	01336b2d3e8d3c08ca085d6fbf91ea03
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsFriendlink.hbm.xml	2	ce1e847be74ecb632a237bf7e36d8432
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsFriendlinkCtg.hbm.xml	1	c821b5e943e8253f1f7193e46a752709
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsGuestbook.hbm.xml	2	66dcc174f96232efe27ac951fefa47ee
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	34336c85796f5a4a3dc694cd27cafcf8

ms/entity/assist/hbm_oracle/CmsGuestbookCtg.hbm.xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsGuestbookExt.hbm.xml	2	1997712ce98b1325ae08fd0c8c1b9a2e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsKeyword.hbm.xml	1	33c709d02b6c7e933cf0dc5d8ed3db2e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsMessage.hbm.xml	2	5c26e2783a38193ee674712e2ce109a3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsReceiverMessage.hbm.xml	2	27a16419cc3a1047b68270a88aaa021e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsSensitivity.hbm.xml	1	8f89158f27bb74ab9cb36594c3f2d434
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsSiteFlow.hbm.xml	2	b7f232d9138169d0763cd609ba3401fd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteItem.hbm.xml	1	e2f552f583a6b6eb4ec105070a95528a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteRecord.hbm.xml	1	b50ad1d53746b3f0d37414a60d3c8f61
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteTopic.hbm.xml	2	076b3fa6ebf41428c237c431da3fd7f5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAcquisition.hbm.xml	4	07a5e3c23419a4a2e1c87d5d306aad9a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAcquisitionHistory.hbm.xml	1	0da9d1db0700aa1a198d588735066e67
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAcquisitionTemp.hbm.xml	2	2978ec00c26bfa28139fa19ceaefe613
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAdvertising.hbm.xml	2	e3584b9e58472f5a7e89879ff2ce865c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAdvertisingSpace.hbm.xml	1	ec3743970cf9703c13c29274e94e3e7e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsComment.hbm.xml	2	d973053ed2b25bd98059ac9a559d7244
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsFriendlink.hbm.xml	2	cba76d4ee7fba07d9e711d60ba1d94c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsFriendlinkCtg.hbm.xml	1	9bb5af460f6862fbbc863d7df4d84402

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbook.hbm.xml	2	27b1010d765e930656f8e02df8edd6ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbookCtg.hbm.xml	1	91c737657cc3c0e9b5755a4f52fc3dae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbookExt.hbm.xml	2	1997712ce98b1325ae08fd0c8c1b9a2e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsKeyword.hbm.xml	1	4f17d895cfc2019616fe9b298e518408
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsMessage.hbm.xml	2	18af079d549e1025c224258256d999d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsReceiverMessage.hbm.xml	2	12063a668e2a3002525b64b0bedea9ae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsSensitivity.hbm.xml	1	45f7f7f8cc500f1d60535bcd26a0b241
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsSiteFlow.hbm.xml	2	09b3ba5c720b6073b213298cf26d939e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteItem.hbm.xml	1	a5d8598ed2b4823c8e6d69ee2236caa0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteRecord.hbm.xml	1	f6ee83f7726df69e9d0fc3a7120533e2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteTopic.hbm.xml	2	5b973992faae627b6e008e62177b691a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseChannel.java	10	18a3cca3f4423eb3ff46e5ba544ba0c1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseChannelExt.java	16	f2bdd0de9bb5f050c26227886d98540b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseChannelTxt.java	4	80b67ff53e0e51fe7b5d85e0fa27ba73
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsConfig.java	10	de197b9467fca0f11febd6987a433af9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsGroup.java	7	27f6f89eecb4738a1c8b65914d202258
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsLog.java	6	2406c2ee0ba4c8b85d88d2a075bc84f7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsModel.java	9	d558333ba536eaab06372b00283f4c8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsModelItem.java	9	a90db870c73644fb768b5310c2ecfedb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsRole.java	5	f1ddae8d9eb0288669d1fe546416d57c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsSite.java	14	8acdd37c69a96c6be552347e849da672
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsSiteModel.java	7	9971bb2564997ee047ba0531e0a6abdb

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsTopic.java	7	41fda3ef86a3135eaa331de4f1c14a5b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsUser.java	14	8e829a0f6ebd6daec74f0d331e78cb74
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsUserExt.java	7	b624447268d254c550114bfd6a48db72
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseCmsUserSite.java	4	aea2267a5fd9c2d6363327a57332f5d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContent.java	14	86ed27001061f094752eb8837e46ad10
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentAttachment.java	3	68a7bcc4d281a865418831cb61bceb20
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentCheck.java	4	9c45776797249b085d619479fea98759
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentCount.java	11	8b6227a63ad5105dcbe4cca8ddae7240
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentExt.java	10	1b80cf40a2e83fb2de001947e39dfff6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentPicture.java	2	9c370bb41fa2b8210b6456353026626c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentTag.java	3	760aacbab063c2b5396837835f9b4bed
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentTxt.java	4	df554e45896d05b017fe820f15f0b5a9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentType.java	5	3340b2a74b13c38ad88a9209fd0ef82a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseEmailConfig.java	3	6a660fa8df090bd97b6c99332f843df4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseMarkConfig.java	6	489197e86a2576060dc4d319e5175c62
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/BusinessCouncil.java	2	12ebe91975a3bcebdf5c70f79258ba76
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CConfigBase.java	2	308453d6ce4eb357ed4e9da63a8242a7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CCooperateBusiness.java	4	c2471dac84d251835974e84b7f0407ce
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/Channel.java	17	f5272406ec4c98f07b7c9416e95cbc31
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ChannelExt.java	4	458298e01747d8fb900750322b45d9d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ChannelTxt.java	1	6c2ece50dfc137c9ee74cc876388e369
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsConfig.java	2	ed28a8fa16adc615576f7efa84e85cea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsGroup.java	3	5b90a1a83d904f7a1c4976d886278a0d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsLog.java	1	f2667b747bed30d491bef44308cbf057
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsModel.java	3	7e7dfca72e9a0d727409ed975cdfc05e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsModelItem.java	2	d3a40b0a15ab24578f7b2af60ffc67fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsRole.java	1	4bbbbccaf6aecaf45fb6856761c30811

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsSite.java	6	460d1dbcb1f8e043fd87057d084a05d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsSiteModel.java	1	1b9333955dedadad62d27799b6bd8c96
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsTopic.java	2	5500062e904b2ffa0f7af0708d4fe835
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsUser.java	11	bec7379112e2a7af7fac62a247dbb680
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsUserExt.java	1	5b862616cf53721f26fa45b535945d45
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CmsUserSite.java	1	f9cc401093a458726b2c32ae1ca5d258
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/Content.java	19	489d8c5d12c637f1d12f1320bf383ef9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentAttachment.java	1	912184029cc4cb77decc09a78ff8c3f8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentCheck.java	2	14107af5f7ab74f7e0f3d047fceba802
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentCount.java	3	b83f0969d35c91d824b77e036bc2976e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentExt.java	3	289f8b478a03e57985f0a3e8230985cc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentPicture.java	1	8b2da9b73856b0b3157431ffd004e8d4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentTag.java	1	68a60e1e2c00750207170527e0552888
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentTxt.java	3	d54dd780f4dcea138f9dc763fcd0684d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ContentType.java	1	e97b3dd55bfa361077a6ca60749305f4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/CoopBusinessTotal.java	2	60a43ee7356c25c434d401aee2ee9bf0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/EmailConfig.java	1	d344cb2afa35fd6724e30192dce0ad14
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/FormPropertyVo.java	3	463269526a87db9139deb8440b88b48e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/GongShangweifa.java	2	0256cdb8ec6667ad130dcf0bc7f29198
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CConfigBase.hbm.xml	1	929faa5c9ef04303eda2e7f275c69235
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CCooperateBusiness.hbm.xml	3	e681146fa5777d16d843bc8f30d2b3ea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/Channel.hbm.xml	3	ea4fe624593381f3c116ea86a1f5346a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsConfig.hbm.xml	4	f9a649ca7c61a6facb0c6fcbb2cde78f

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsGroup.hbm.xml	2	e179c70d8a4479bf0bfd11e6d166bf25
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsLog.hbm.xml	2	2a0f90e70ef09b960fb2d81e7a270ca2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsModel.hbm.xml	2	ee231e0577df57deaf4798759a1f6bd9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsModelItem.hbm.xml	2	7032c86c11f151abf30c5b941b2f1ce9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsRole.hbm.xml	1	4c2e29d04a1ded2dfe24258d9fc14ddc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsSite.hbm.xml	4	400e5a8ba60ee446ce6061a9b2e87551
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsSiteModel.hbm.xml	2	5ef6ddac5c964aa0ca75578d87552c29
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsTopic.hbm.xml	2	86708219f6f6dca55a740f98058f2953
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsUserExt.hbm.xml	2	31471fe2cf210c9b85048f8367826449
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CmsUserSite.hbm.xml	1	97eec5a8dba6360115e5aaf246ce3159
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/Content.hbm.xml	5	18602e68f5a6d43a3e6a64707b68944b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentExt.hbm.xml	3	8fbf3703a4884ecf1e13348a6985a636
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentTag.hbm.xml	1	7834e5a998303b0c3f727bc4cf4a6d9b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/ContentType.hbm.xml	1	4376595eacc3207c544b24c5518714f2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/CoopBusinessTotal.hbm.xml	1	2b1c838bf4024be5fefd6c454312a788
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/SpaceAttachBase.hbm.xml	2	1ae022795b8cad8162f14be0f05a5d8c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/SpaceCertInfo.hbm.xml	3	b7190fa914e299df214c37d6d55608c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/SpaceClxxInfo.hbm.xml	3	d4a9253dbd203d8cdd15645d5003c9d8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/SpaceDataExtend.hbm.xml	2	96b446aa2e6abb86605e21e8ea735cc0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsAdvice.hbm.xml	2	81a184010382c24ca6271f667ba14cd2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsBusinessTotal.hbm.xml	1	f9eb242d965581d2d3b7e04f46afcaa9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsWebhallBusinessInfo.hbm.xml	4	97b7dbc188b721a6cec75e05d388a62e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TInsYwpz.hbm.xml	2	e6cb612824700fbc78873ca7f1b0c8d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TOpinionRecord.hbm.xml	1	129453867efa701f7c0641bebd612bf6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TOpinionTopic.hbm.xml	1	da7338bdc1b1cf283dc7c09b9cf55082
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TShareCertificateinstance.hbm.xml	3	1b9eecea2426ea815ce784fd2b56af59
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TShareFile.hbm.xml	3	110f4c480c7dd3de4e8aa64e05c15a7b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TShareInvest.hbm.	2	3824f18bf0f16303fe2bd08bd8ee2d3c

xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSharePermissionitem.hbm.xml	15	3e1d61363152e7392c77825de1494ac0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TShareWebCondition.hbm.xml	4	38a3953f00faac1c212d267a219114ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSpsxPermissionmapsort.hbm.xml	2	9ec62c5e7e823577a150f701cd9e7446
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSysDeptWindow.hbm.xml	2	3c4e3171bb02d2b514dc666dd3ecf4cf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSysRegion.hbm.xml	2	38c5624390bba6a12dbec5c4cd6655c8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebHallIncInforMation.hbm.xml	3	b4a99022c3ef3f8755bbda6794ced19c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebhallReferComplain.hbm.xml	3	23cc7fad44d1e409ca611a430951ca56
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TWebHallUserInforMation.hbm.xml	2	b9ef8114fe33b802ef23b76de323f24a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/TXmlClob.hbm.xml	1	9dce5aae665669d2fd1a249715de1fb6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VCooperateBusinessinfo.hbm.xml	2	cd025c7add95ad2c15fb66a19bd23729
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VShowPermissionitem.hbm.xml	3	1bf43a7b039ea14d8dd958775997c06a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VSortPermissionitem.hbm.xml	3	4a5ee4532323ecc6fe89c9e0e4899586
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTInsAdvice.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTInsBusinessinfo.hbm.xml	2	f2032c1dd0bedd21996511cce64d5993
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTInsWebhallBusiness.hbm.xml	2	6e68932acb17dfa7ba26cc72ff032d5e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTSharePermissionitem.hbm.xml	1	d919f25276bfb4ce08a8c9a364c06881
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_db2/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CConfigBase.hbm.xml	1	0a4a6f2001cb6cfe28969daf5e8de6a3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CCooperateBusiness.hbm.xml	3	89d84427f3ff60de2b1580d723f0ce98
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/Channel.hbm.xml	3	6de5e4fdf96deaab9775275a6f7e90c2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/src/com/jeecms/c	4	d02dc141778e080e7aff27a2ab81d38

ms/entity/main/hbm_oracle/CmsConfig.hbm.xml		b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsGroup.hbm.xml	2	0387220e2d89c3af5b9a5c973319d4c3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsLog.hbm.xml	2	cdda119e1dc5fed30c7651862c01c25e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsModel.hbm.xml	2	0fc7f191a04a8b140108c7dd58e1fcf4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsModelItem.hbm.xml	2	4137a13e8b6be0a1fe17c8f30799094b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsRole.hbm.xml	2	76320a9a80a1cef2bdbea815252af760
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsSite.hbm.xml	4	d33c333fee35a3a15cb16d97692fd72c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsSiteModel.hbm.xml	2	22cd375f7e7315d1e987c0baec1d440a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsTopic.hbm.xml	2	a738f01cde50a9351e0702544868a2fb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsUserExt.hbm.xml	2	31471fe2cf210c9b85048f8367826449
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CmsUserSite.hbm.xml	1	737056e2b2956c265636afc9f5f5e060
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/Content.hbm.xml	5	9625468c22cf5dc29eb553d9a9fa2f61
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentExt.hbm.xml	3	8fbf3703a4884ecf1e13348a6985a636
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentTag.hbm.xml	1	4bcb608317ca65f9e8c1fea48e49d9ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/ContentType.hbm.xml	1	32c49d639a686204912e94d0e2ef1170
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/CoopBusinessTotal.hbm.xml	1	4d2683310d9d9fc22b26f8b18692e3f6

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceAttachBase.hbm.xml	2	70c32e40bfa6321f0d6d37520a4d6f83
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceCertInfo.hbm.xml	3	66cea0d23572bdf0824e8cd68360efee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceCertInfoExt.hbm.xml	2	ce97858edc9763dcf5a7f70b53d11d6d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceClxxInfo.hbm.xml	3	4f990996bed68f1b8bed0bb9a5e0821f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceDataExtend.hbm.xml	2	c7e1646f603916e0710b364ecb22b976
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa002.hbm.xml	3	936327bfde3c1ea5ed22a77606388813
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa003.hbm.xml	3	858e33bd3597ca95521a98b5d41e97aa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa004.hbm.xml	2	fa6d7a8da6a6055a5ba5bf34e777a133
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/T29e000028aa019.hbm.xml	3	0142d8c5ac236cb5cdb872f2e172b378
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/T29e000063aa003.hbm.xml	4	27ce6a8da5ab99dd292a4a2f497185d6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TFormLib.hbm.xml	3	4c033af8733dce812bf38b03deb8e323
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsAdvice.hbm.xml	2	e3dd95512190fda7897fc4d3889e64c5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsBusinessTotal.hbm.xml	1	d9078e4826fcba68e5273f598780d96f

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialCompare.hbm.xml	2	030eb0a851457d3bc305c439851ecfd7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialValid.hbm.xml	3	857827b16891b336f663085d07dbbe22
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsWebhallBusinessInfo.hbm.xml	4	e2b0c1fd0302b4d45ba7a52ab248390a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TInsYwpz.hbm.xml	2	71dc96cecfb5febaf7c855952d83e096
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TOpinionRecord.hbm.xml	1	e2b8a4dd299de9b92db1305e35f39559
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TOpinionTopic.hbm.xml	2	0f52f159dad1d710cc24e41322276fd0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareCertificateinstance.hbm.xml	3	ad09edbbbbbdf23dab883cef080ece1b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareFile.hbm.xml	3	cc06dc13ae02bb25cef6fec9c7decb62
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareInvest.hbm.xml	2	3824f18bf0f16303fe2bd08bd8ee2d3c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareJdsqxx.hbm.xml	2	80cd71e6de5433facf3a15a5f5d8880a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSharePermissionitem.hbm.xml	16	be66152191dc5fcab41191e3fa941138
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareSxclgl.hbm.xml	3	e0990991d71bb3ed13988f9671bf9e1c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TShareWebCondi	5	90873f1ca3c1a0cef2dbb4af61e859dc

tion.hbm.xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSpsxPermissionmapsort.hbm.xml	2	a85a34840760da1e5fc80fc95ca47ab7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSysDeptWindow.hbm.xml	2	ec7cfe18075ae6960af74c4ee6621311
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSysRegion.hbm.xml	2	38c5624390bba6a12dbec5c4cd6655c8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebHallIncInforMation.hbm.xml	3	67c29bbdaf568cca9244228d2623b216
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebhallReferComplain.hbm.xml	3	97b8c7e8d3397afa8fbdbbe026d4342c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TWebHallUserInforMation.hbm.xml	2	f77c7005edbde91ff3b0fda80dda5e56
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TXmlClob.hbm.xml	2	7ff0ca5eff979e507965e3888b34b275
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/TYWLSHLog.hbm.xml	2	989640db89b06daff918e0b9b91d2a38
/WebHallCMSV3.0BAProject/src/com/jeecms/c	2	69d500b40eddb6a005261b669ddf1c

ms/entity/main/hbm_oracle/VCooperateBusinessinfo.hbm.xml		5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VShowPermissionitem.hbm.xml	3	92e06dec08919fa693a3ff7aa9237e5c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VSortPermissionitem.hbm.xml	3	34ba0c4aafdd5b98c5f5dd223e63024d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTInsAdviceTJ.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTInsBusinessinfo.hbm.xml	2	a7731bde4a30a11a9b9a7f2ad6fe2598
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTInsWebhallBusiness.hbm.xml	2	6e68932acb17dfa7ba26cc72ff032d5e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTMaxsxbhPermissionitem.hbm.xml	1	c7600d78cdcfdb04eed46d2e58f481ca
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTMaxsxbhSortPermissionitem.hbm.xml	1	916992c20ee951b1a4e6c44c80da5620
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTSharePermissionitem.hbm.xml	2	7daff06d1980f82253fb60f7057c8ad9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageChannel.hbm.xml	2	e624b1ac4037a6d6f377a5795bd239ae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageChannelgr.hbm.xml	2	72ba436cb1dd2c7f113eda5167f0c733
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageEnterprise.hbm.xml	14	42be8f9a3548a8c2d252be8955b1970e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageFavorite.hbm.xml	2	471a89abe4055df27cee3a677a770b29
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageFavoritegr.hbm.xml	2	3874bae82a54dde5a48348685002affa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageReminder.hbm.xml	2	95763034d58f700c5d240fd992137785

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageRemindergr.hbm.xml	2	28c4491d6c2fbe3b6a55ba99d59b4d4d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageUserChannel.hbm.xml	1	e00da79034193da17867466c2f8f618e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_oracle/WebpageUserChannelgr.hbm.xml	1	b93278cfce880bf625610bff081f553b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CConfigBase.hbm.xml	1	0a4a6f2001cb6cfe28969daf5e8de6a3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CCooperateBusiness.hbm.xml	3	89d84427f3ff60de2b1580d723f0ce98
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/Channel.hbm.xml	3	ea4fe624593381f3c116ea86a1f5346a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsConfig.hbm.xml	4	f9a649ca7c61a6facb0c6fcbb2cde78f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsGroup.hbm.xml	2	e179c70d8a4479bf0bfd11e6d166bf25
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsLog.hbm.xml	2	2a0f90e70ef09b960fb2d81e7a270ca2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsModel.hbm.xml	2	ee231e0577df57deaf4798759a1f6bd9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsModelItem.hbm.xml	2	7032c86c11f151abf30c5b941b2f1ce9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsRole.hbm.xml	1	4c2e29d04a1ded2dfe24258d9fc14ddc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsSite.hbm.xml	4	400e5a8ba60ee446ce6061a9b2e87551
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsSiteModel.hbm.xml	2	5ef6ddac5c964aa0ca75578d87552c29
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsTopic.hbm.xml	2	86708219f6f6dca55a740f98058f2953
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUserExt.h	2	31471fe2cf210c9b85048f8367826449

bm.xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUserSite.hbm.xml	1	97eec5a8dba6360115e5aaf246ce3159
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/Content.hbm.xml	5	18602e68f5a6d43a3e6a64707b68944b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentExt.hbm.xml	3	8fbf3703a4884ecf1e13348a6985a636
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentTag.hbm.xml	1	7834e5a998303b0c3f727bc4cf4a6d9b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/ContentType.hbm.xml	1	4376595eacc3207c544b24c5518714f2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/CoopBusinessTotal.hbm.xml	1	4d2683310d9d9fc22b26f8b18692e3f6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceAttachBase.hbm.xml	2	dee69b99afbfd65ad83dd8bc3f25361f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceCertInfo.hbm.xml	3	b7190fa914e299df214c37d6d55608c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceClxxInfo.hbm.xml	3	d4a9253dbd203d8cdd15645d5003c9d8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceDataExtend.hbm.xml	2	df036f11865f9d02765a53dc91e02272
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/src/com/jeecms/c	2	81a184010382c24ca6271f667ba14cd

ms/entity/main/hbm_sqlserver/TInsAdvice.hbm.xml		2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsBusinessTotal.hbm.xml	1	d9078e4826fcba68e5273f598780d96f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsWebhallBusinessInfo.hbm.xml	4	97b7dbc188b721a6cec75e05d388a62e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TInsYwpz.hbm.xml	2	e6cb612824700fbc78873ca7f1b0c8d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TOpinionRecord.hbm.xml	1	129453867efa701f7c0641bebd612bf6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TOpinionTopic.hbm.xml	1	da7338bdc1b1cf283dc7c09b9cf55082
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TShareCertificateinstance.hbm.xml	3	1b9eecea2426ea815ce784fd2b56af59
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TShareFile.hbm.xml	3	110f4c480c7dd3de4e8aa64e05c15a7b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TShareInvest.hbm.xml	2	3824f18bf0f16303fe2bd08bd8ee2d3c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermissionitem.hbm.xml	15	cf36ebcbdd4c6455a2300ab1ca8fd224
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TShareWebCondition.hbm.xml	4	38a3953f00faac1c212d267a219114ac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSpsxPermissionmapsort.hbm.xml	2	9ec62c5e7e823577a150f701cd9e7446

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSysDeptWindow.hbm.xml	2	3c4e3171bb02d2b514dc666dd3ecf4cf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSysRegion.hbm.xml	2	38c5624390bba6a12dbec5c4cd6655c8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebHallIncInforMation.hbm.xml	3	e670baaaf0af3acccdd927c90cf89757
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallReferComplain.hbm.xml	3	23cc7fad44d1e409ca611a430951ca56
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TWebHallUserInforMation.hbm.xml	2	b9ef8114fe33b802ef23b76de323f24a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/TXmlClob.hbm.xml	2	879f436d3ced838eda9b6074464707c4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VCooperateBusinessinfo.hbm.xml	2	69d500b40eddb6a005261b669ddf1c5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VShowPermissionitem.hbm.xml	3	1bf43a7b039ea14d8dd958775997c06a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VSortPermissi	3	4a5ee4532323ecc6fe89c9e0e4899586

onitem.hbm.xml		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsAdvice.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsBusinessinfo.hbm.xml	2	3127d38279c8234fdd40f64601fb701e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsWebhallBusiness.hbm.xml	2	6e68932acb17dfa7ba26cc72ff032d5e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTSharePermissionitem.hbm.xml	1	d919f25276bfb4ce08a8c9a364c06881
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/hbm_sqlserver/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/MarkConfig.java	1	31e729ecc09f6f19414233ed2a22327e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/MemberConfig.java	5	70d6991de0ab10b3a43a0d2e5940fb8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/QRTZ_TRIGGERS.java	5	95d6710cc6840aa26d56d2df779e48ad
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/QRTZ_TRIGGERSID.java	1	7142d9b4741dbe591f22c3daa177f7b4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/ShareInfo.java	2	4431252def2e18e9a5f4994505a2ec06
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceAttachBase.java	3	d4c09c4f94e7f1b59cfc362df701b1b0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceCertInfo.java	5	9d3a55a961bb688d0887ebd254aef13b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceCertInfoExt.java	1	b1e0ff4fa4ee29b9afb10a88e1c87b32
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceClxxInfo.java	4	b216b22fb464af8b1c25fccf68047a92
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceDataAndValue.java	2	d83aef7e7adc6de39cae22ef7283637c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceDataExtend.java	2	e306fbdd7fea6701b86c9ddfed080b32
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceDataExtendValue.java	2	0ca914cfde24f7266b94f08f093dc4b2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java	3	6a1bd33166fcbe4aab1cf107e8fc3c4d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa002.java	6	fad08dd86fc9791f86d55f2145675d70
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java	5	25a2b164154e973c4dac7ade71a9707c

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003Id.java	4	4c2940099fb79e88accb838319b19eb1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa004.java	2	0287d5c9b1c5324ae466dd6ab3e96929
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000028aa019.java	5	9da1f059a108eb485cdc5549cc807c48
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java	5	d81d566879af38bb75781aff64716950
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003Id.java	4	f8264d454294bc1555a80e898f1a32fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TFlowNode.java	5	b0d0c8dbdc7be411e6909beeb382b698
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TFormLib.java	7	69acc82c701e734e1776bc1bf4605f3c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/THrUser.java	10	d4135435649951dd3bd8a312ed333563
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsAdvice.java	3	50b31869f23314489868d49e3f76c2f7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsBusinessExt.java	2	df5f55505d8e2fbab1eb959eef1d5786
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsBusinessTotal.java	2	5b9d160f02596a4de21ae378a6e1ea40
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsFormData.java	3	40d21eeda7375175518da0feaa038525
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsLogTysp.java	3	211a6fa13ef235458c92bd1698d39098
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsMaterialCompare.java	2	567613b6c3a2c321040c15e553b0b374
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsMaterialInfo.java	2	155301272a187b16fb86026fb739ed46
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsMaterialValid.java	3	54b2f22da857036fae18a02b046367b2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsWebhallBusinessInfo.java	4	b878cffd1c249e8346c0301ea8bb3688
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsYwpz.java	2	c749bc0cb45a3b4a98060a0c878ee66e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TOpinionRecord.java	3	0f8c2e190559a34137b1d7e243351597
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TOpinionTopic.java	2	013ad8d8e555d2e0188b9e0a6b9a930c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TQzqd.java	8	9881e5c00376441c83a768fe9ccbf797
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareCertificateinstance.java	3	bec1a0bab0f7257098844495c995e2ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareClxx.java	4	19b3ec8bc53b8ed9f87cd76b0bde73e0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareFile.java	4	774b49242193235923ab33064834aaaa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareInvest.java	2	063d66b028de7c3c45d995fefe7e3f43
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareJdsqxx.java	2	11611322f797646d090d23271fdbdf24
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSharePermissionitem.java	15	05764e41e4b3b125f3451da9bdfb498c

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSharePermtowindow.java	2	41ab1592253c871fb070fb20cec9a16f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSharePermWs.java	2	eaf0b314c15e6bc4402189198372b8c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSharePost.java	2	5fd944b3dc6abf407a4ed66d55dd6d61
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TShareWebCondition.java	4	abe9a8fe773f477d5f38267a207b27d0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSpsxPermissionmapsort.java	2	8c43eb1ecaff4b6179a2fa7eadcf791e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSpsxPermissionsort.java	2	c98fd6481fd5e8a600643fdd925b9169
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java	7	87584d25eb115889b9ed7af8470dd1bd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDeptWindow.java	2	a2e32dd98ffd091462fbf1d889374d43
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysFlowlibmapform.java	1	77aa23d5e24a03f64fd6d9823b023f5f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysSync.java	1	ab99890d7f6f20fa19732ef775d37f44
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TTyspBusinessInfo.java	4	20dc628ff2de13df633c03f73982a59c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TTyspGrsbclxx.java	4	3224c7d0c20ad9eca29368985440e701
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallBusinessInfo.java	3	23d2764df7a05042f2c3f71b3d2f8326
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebHallIncInforMation.java	9	99a8f81f29bc4dcfedec83490c726b09
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPermissionitem.java	1	6290272ee0d6a74fa494d4707c79c9cd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPermissionitemPost.java	2	430e4ec12ccf9e166011b6d370a53346
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPost.java	2	45186c9f84370f4b905108fc599fc5de
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallReferComplain.java	6	343f0e6b6ff24a423f3e0faf22119bd5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebHallUserInforMation.java	6	82325ad391928ea0dbbda5d7d16ac6f1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TXmlClob.java	2	5620a035506e099b958397b540860d96
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TYWLSHLog.java	2	5e22e8b489f8d0cbaebbf876e4154962
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/UserFormVo.java	3	c7666a7474151de2a0bf2796b58bdde0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/UserVo.java	7	4107dfc3b360858ec0d0198b95690172
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VCooperateBusinessinfo.java	3	857a9451a6c1cfb7be195be7efd03c8f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VShowPermissionitem.java	4	5eb7eda61a0cee623b2a0a0e248e1a9c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VShowPermissionitemVo.java	2	51bda864ff8e7a38125dddb550120a2c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VSortPermissionitem.java	4	10083f5989b025902102e6fd6a199e54

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTInsAdviceTJ.java	2	195452eab7af9c43f95b63c9d79b90c9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTInsBusinessinfo.java	3	b4053d140b0eba54a8416bd9186e85be
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTInsWebhallBusiness.java	3	f3cd484c3f50a989d5bcb751c761d818
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTInsWebhallBusinessTJ.java	2	f95e31ffcc32a6147d6c47b06780fdc9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTMaxsxbhPermissionitem.java	2	4718a05e0550071c515260ae4e193440
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTMaxsxbhSortPermissionitem.java	2	ef0cea689a3dd56e11039785da3c7354
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTOpinionRecord.java	3	c3e8974d84ba293663debbc891d75815
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTOpinionTopic.java	2	539b1516b01d25c0632d5f57ac6ae254
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTSharePermissionitem.java	2	0f5a30cc26d07a5161cb2fc25b4fe905
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/VTSharePermissionitemType.java	2	e0d25bcc823c940c78247714c5835cbd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageChannel.java	2	b35ed199b615a74bbcdfe4f54752a68f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageChannelgr.java	2	eece8bf6b9ce92fb8fd8ce03bb99b4ef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageEnterprise.java	114	85112bcaf0169d10d1d44871204a86c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageFavorite.java	3	ad1f18873d62142f753959f853158e13
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageFavoritegr.java	3	61fa7c48fcdca8a0ebbb7de75d9fc41d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageReminder.java	2	a11aa8a64be532b9b37f8edd505d8996
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageRemindergr.java	2	0dcc7575667fa407711c2d2d749ce4bb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageUserChannel.java	1	55320c16fc4b1ac6967df336c19eb9c9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageUserChannelgr.java	1	4cca11d14c170ae98846dfa9d9cb90ee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/ExGongshang01Qymccxxx.java	15	44252c66889cb75dc9826f7b7852724c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/ExGongshang01QymccxxxService.java	2	a6bd964a2bbf6b39b974f7c709fabd84
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/ExGongshang01QymccxxxServiceImplService.java	3	121ced10329c6eac4b455f33a0fa5e45
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/FindByHQL.java	2	459b8365feb110c04f8cc1e431e57f40
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/FindByHQL	2	c5e9a565fd48286094831cefc8a50d19

Response.java		
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/GongShangweifaTagDao.java	1	8bdc6d968a3e8830ccaf8dc936001478
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/GongShangweifaTagMng.java	1	b02a5bb1c136906a715ba54e05d512ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/GongShangweifaTagMngImpl.java	1	706051f041eddbeda334cc617f63ecee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/impl/GongShangweifaTagDaoImpl.java	2	8cb43ac914265948e86eff2683e52e10
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/ObjectFactory.java	3	9de5620dfbc950e31f9219993f03ce8e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/package-info.java	1	f00f363164f583dda518921888e0cbb6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/ExGongshang10Qymchzxx.java	11	d879229f33e5c6bb63f6ae7f3ed74de8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/ExGongshang10QymchzxxService.java	2	32992fd2b0a6ae1d984a616dd0dd9db7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/ExGongshang10QymchzxxServiceImplService.java	3	9d9b38abbaf5eb1522cd3316ca038f8e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/FindByHQL.java	2	43a45d91c1eae0d7df0994eb68013b63
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/FindByHQLResponse.java	2	22207925b82fdea7656bdeb7724d0f5a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/ObjectFactory.java	3	2eebab056302caf5acba24344a7fa50c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymchz/package-info.java	1	f7fb3214705ce16d82dcbcd45a8e8d0b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/vo/WebServiceConfig.java	2	dd066c5668a2676bd893fc4e83cdfd75
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/JsonUtil.java	5	793dbe005e898c33045d61be2349a044
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/ContentLuceneListener.java	2	594e43345b6075574bd128175af1e971
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContent.java	6	14923d07edac01fc0c977a5b95873d4d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContentAct.java	3	7c41d6dae5739616aecd7b3c1843d848
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContentDao.java	1	93492b70c09aab64ee6e998d9ea0edfd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContentDaoImpl.java	3	f4bfca80b674661dbc8b90d095526223

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContentSvc.java	3	33d5d483ee9d8944d5c3da1f45af2d6f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneContentSvcImpl.java	8	869496744800e5467a504936371f2abf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneDirectiveAbstract.java	2	80e0db19b34291ab70ee7ced958dd429
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneDirectiveList.java	4	adbe77575141bc565f8a92d2c0334a39
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/lucene/LuceneDirectivePage.java	4	7390a71c286deec82ab4b9a06930f93c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsAcquisitionHistoryMng.java	1	20a4b1a4551aff554e8c6eeb287e4bec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsAcquisitionMng.java	2	3753e3603cb8611cfc03112a28ce2b7f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsAcquisitionTempMng.java	1	97e8b2dee24c9f0805ba4acd808adf6e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsAdvertisingMng.java	1	3eda89174f3785e1d6541c904da8e3d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsAdvertisingSpaceMng.java	1	6e4f74d6100c71b12ce5f34bdb369743
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsCommentExtMng.java	1	f4ab70b9a6573c92ca486c1fb046922e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsCommentMng.java	2	751e6defaef658f55e83691178bc6d97
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsFriendlinkCtgMng.java	1	b9951ed5be284cf09aa55cb7a7b965f2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsFriendlinkMng.java	2	7d1b24f90fdec17d6050c6eaef4a92e3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsGuestbookCtgMng.java	1	18bddbe432e2277247fa1e2549996929
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsGuestbookExtMng.java	1	3ff49a0588a71c28d7c5f4e80914d9b6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsGuestbookMng.java	2	fab0bdcbb8eb2da6dbdec95d4d3fcd16
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsKeywordMng.java	1	11a2ab21cfceeafb642e46f72e77e62b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsMessageMng.java	1	ed941496bb93a7310fcf18c95aa7cb4d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsReceiverMessageMng.java	2	aaaa97f2a6a926a15338af879e459e2f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsResourceMng.java	3	b895ecf9ec323d9aeec9093209dd5b08
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsSensitivityMng.java	1	1c2d2f4651431f2a8ac92277ea2e8358
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsSiteFlowMng.java	1	de437a596e1cb55b501ae3a787d495fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsVoteItemMng.java	1	a481ab85046686cf0643a6f70747aee7

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsVoteRecordMng.java	1	7e918e1800585e7c33ea256d6369f448
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/CmsVoteTopicMng.java	1	4da89000c2ebe438fc2707b17709dd20
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsAcquisitionHistoryMngImpl.java	3	5257e3f0f37ae95585cbef2393318298
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsAcquisitionMngImpl.java	8	242fcab83cc5e46cbd974f98f4ba0fe5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsAcquisitionTempMngImpl.java	2	c640ae590ada0c37bab959415f0ae855
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsAdvertisingMngImpl.java	3	24ad7e69077702a094f5733d23f524d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsAdvertisingSpaceMngImpl.java	2	4e9845cb20d0e257eda8181a087ce23a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsCommentExtMngImpl.java	2	777e372b2d99007e473206ad644f859b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsCommentMngImpl.java	6	d751a56bd1021acdca366967c79d446f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsFriendlinkCtgMngImpl.java	3	27757a49cc99d42c5533d1d8f1336604
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsFriendlinkMngImpl.java	4	c0dc235a7f3e66cdbc3f830ff125ffd3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsGuestbookCtgMngImpl.java	2	75e23b0323d005a5d04d8e58bc196cb8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsGuestbookExtMngImpl.java	2	840ff328c7691f94308466ee14e19062
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsGuestbookMngImpl.java	4	9068605ddfadc0abc9bb48bd9ce8de87
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsKeywordMngImpl.java	3	f6570f4f39ca53698aca918bb7023e62
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsMessageMngImpl.java	2	31a05e8835e5212a9974d288177fdbd9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsReceiverMessageMngImpl.java	3	aba572f68671c2da33c945575a0c782a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsResourceMngImpl.java	7	d761e52ee4bcbd9014094f001b6c298e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsSensitivityMngImpl.java	2	adc828dbd0cfd023cd186c881aeca1a8
/WebHallCMSV3.0BAProject/src/com/jeecms/c	2	d6aaf306cbc4e1e0b3ed474bf3c6560

ms/manager/assist/impl/CmsSiteFlowMngImpl.java		4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsVoteItemMngImpl.java	3	59e02ecc29c10945d72cf5684b5553d0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsVoteRecordMngImpl.java	2	42663d8c43bb9c42a87ae0627b6ab8df
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/CmsVoteTopicMngImpl.java	4	bb534cdbe79d261b12c88e5e752ed794
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/impl/TYWLSHLogServiceImpl.java	2	4e89c08846780fbc8bb252823d6fa3f9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/assist/TYWLSHLogService.java	1	d768fdf4b6878f0e5e0e4f102244c025
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/BusinessCouncilMng.java	1	35398dfb01fcb998f98d2a209e089f52
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/BusinessTagMng.java	1	ffb20a6a761787a3bf563483daef5faf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/BusinessTotalMng.java	1	1c1906c174c2b33cb2fe1733660a03eb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CertificateinsMng.java	1	105d6c8cb70bc4e98e8208a9c6821749
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ChannelExtMng.java	1	33c10bf4145523e0f555a8aa1a7d159d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ChannelMng.java	2	e3b7b218adf8a315cc0e5fa3453aa665
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ChannelTxtMng.java	2	bc2653fe43bbe9a25562d6d3e7177b83
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsConfigMng.java	1	cf4917e41e9772118d2ad11fe4764252
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsGroupMng.java	1	de4361d75437153096e6fc0c4b7e7524
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsLogMng.java	1	b6f1eed59c22a07918d8980855f5e5f1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsModelItemMng.java	1	1afcfd67a46d51325fa0cd46752a77ec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsModelMng.java	1	892ec1c15b72c906d3be1415e44370b3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsRoleMng.java	1	76125e129beeaf39640730d767919588
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsSiteMng.java	1	98d65c2f6a7a67db01556f69a0a4b7a8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsTopicMng.java	1	833027164b373e0bb4d5ae4e6905d7d6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsUserExtMng.java	1	6592db0ea0d881d34f70a71f8fab8dd8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsUserMng.java	4	24b9822b45466c0018b6644f43490ed7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CmsUserSiteMng.java	1	378b3d40b077b2e834558485128b7270
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentCheckMng.java	1	e4b8f40c2ddecfd2a65132fa5b03a94e
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	c77bcb953f9babcd5a00611056eeba0

ms/manager/main/ContentCountMng.java		a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentExtMng.java	1	ff9a0f030b62c3e452b8c5ea3d94614d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentMng.java	6	e4bde2311cbbead5e0fc11b45665678e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentTagMng.java	2	b3230694b0ff01368d2731e144fa6cae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentTxtMng.java	1	4c4f9c062f81ae417f1cc4369e064803
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ContentTypeMng.java	1	bd1231e6be3d5f37f76a9d5e0e016a57
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/CooperateBusinessMng.java	1	041eccd648bbb2f74d3368fc287e9306
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/DeptWindowMng.java	1	39f05a1ee13ae8fccdac211311947aaf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseBanShiTingService.java	3	b7f101e0296c23107df71bd7730ece4f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseBanShiTingServicegr.java	3	0954291b2b21686e343507991d73138c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseGuanZhuLanService.java	3	b141bc144c132e7dfe6d4ba5351bba65
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseGuanZhuLanServicegr.java	3	7c0ab9e567a0b0b423260d0db577b922
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseKongJianService.java	1	a1908b5cf8e8c3119d333080aad951a2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseKongJianServicegr.java	1	a9540c25f43e7588eee54ec910f3e110
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZhengQiHuDongService.java	1	d0eb54b6511db56f9c4f74d7e19536ab
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZhengQiHuDongServicegr.java	1	de95b0a455321626d90156a2b22f6da3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZhiTongCheService.java	1	b7d7b7ed6d3993444ef8407d34305cf6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZhiTongCheServicegr.java	1	9deb9a6e0ecb9ab5e3aa35c7653e0dbd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZiLiaoService.java	1	368f7f19d433ee2f90f31fc8a6e33c50
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/EnterpriseZiLiaoServicegr.java	1	4be22cb3ac211e7b7b68818f5af18cec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/FormService.java	1	316ee7971c781b2a56e3f3cafea06789
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	a2dd1e079a794be7e5314cbf927918

ms/manager/main/impl/BusinessCouncilMngImpl.java		94
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/BusinessTagMngImpl.java	2	0ec3fe4ed80d0741ae65ddf2091d367d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/BusinessTotalMngImpl.java	1	9d2ba7fcfc9527ccd07116cafeb2bf43
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CertificateinsMngImpl.java	1	3ee2ba2a9c1ea025bdd7399434617414
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ChannelExtMngImpl.java	2	51bdff1b259ed7f1c4da3097bcdd6b66
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ChannelMngImpl.java	9	12dd05687d0a8330be51646f5ab8c26b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ChannelTxtMngImpl.java	2	26a3ea8d24113dae180ff898e68870b3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsConfigMngImpl.java	2	f061b760da10ea5a11949e4f26e83643
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsGroupMngImpl.java	2	d7477fe875fff48132440e3728a4de05
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsLogMngImpl.java	5	c8a4dd4e6bcd41485f08a2b4be28d3ef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsModelItemMngImpl.java	3	b8a12452c9e19042d7314d002d04e4b7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsModelMngImpl.java	2	121789da374a5383b0d7d44db3661730
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsRoleMngImpl.java	2	abcb0ab582ce71b883599aff3cbb63bc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java	4	d5b9959c060d931825af2cc7e3420acd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsTopicMngImpl.java	4	bc2323e687e7c79af3a7e792dcb8b5cf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserExtMngImpl.java	2	e360452122cf15c55168d4b9b2ebc46f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java	12	626be1787335b30c0ce0c7749b3dfec6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserSiteMngImpl.java	4	8ca0630917ef8b6ed0543ed801321d94
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentCheckMngImpl.java	1	5f699fa7a8e34002fe55d09d7067394c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentCountMngImpl.java	4	5fa8072a0e595eec249171f9ccf6f4e4

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentExtMngImpl.java	2	772033d6ca3a13283a55df483e30544c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentMngImpl.java	24	9b293cf6079c6c7e56a85b19360c9647
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentTagMngImpl.java	6	e338f36c64b7e7efbfda6650554b7335
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentTxtMngImpl.java	2	ccf3d6376d43a06b65305a541205d836
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentTypeMngImpl.java	2	130ff9896c2a8c642ed02c8fc3519de7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CooperateBusinessMngImpl.java	2	112e47aaba1bd43ef8e35c8d52180136
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java	1	068bb272867a815bfec15722d96b21ce
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java	3	9c0b0a1d2c3c1ba9e615ee4c49614e59
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java	3	1beb046760031bd8d640568dfb3b8528
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java	4	03dc3861cc07b0fd42d77ed9444521e9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java	4	5b4f376b42fe3b570a5df9c6b823b49d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseKongJianServiceImpl.java	2	17b177843ee2fa5dafbfb948656841da
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseKongJianServiceImplgr.java	2	8b95c958f6e1a2ea1a51cdf9eccf492e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZhengQiHuDongServiceImpl.java	2	c9abcdd4476fc12eeb50ee59918803a2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZhengQiHuDongServiceImplgr.java	2	4473bbf047746e0a9b1ba6219c95ae34
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZhiTongCheServiceImpl.java	1	44ae20fafac3ad1cc3303d819b92a7ee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZhiTongCheServiceImplgr.java	1	34c4c927e0d1e736c74d322c7383ff04
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZiLiaoServiceImpl.java	2	0f0765a4fc695b59dbbd9e826f2131f2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseZiLiaoServiceImplgr.java	2	415ee5c7f1e907ffd4a2b010a9b25d91

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/FormServiceImpl.java	22	dcb6dd623d3fe713793bc440fa4b97c9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java	5	4266251b4fee3ebbfaa9244be08b18d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java	6	386cb220a1ad9c51bb834db65f99efec
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java	3	414cc539f498b474c02bc7ed68d3ebb8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ReferComplainMngImpl.java	3	9f61ebca7f909e6ce9aaef43006e01f3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/RegistrationBureauMngImpl.java	2	42305a2ca9a96e873a3bbb716a3514b7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ReservationMngImpl.java	2	9ac101472c583f8b7c5fc8fb2ed26ade
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SchedulerMngImpl.java	10	496e0e08f577cc6df41003f7b57a69e0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceAttachBaseMngImpl.java	2	227a5f4d10c6689f6d9c4e73f54946cc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceCertInfoMngImpl.java	2	64523ba526b16aa36d1d58b81ee68def
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceClxxInfoMngImpl.java	2	11e7d991e2d5dd29408ef1a94e9a5618
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceDataExtendMngImpl.java	1	4e2f7f007175685702b937c66b75a19f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceDataExtendValueMngImpl.java	1	ebacc365ce3db2c7e85c4c4ad8b1fc6d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SurveyOnlineTagMngImpl.java	1	7ca5a2681c9ca609cef201d14988d860
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SyncConfigMngImpl.java	3	c0a82afb20664f754b839658b45f7c82
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java	1	3726594dc67644186a844ebc45e2233b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java	2	19e1b87f434bbea0246825e5fa748e4f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TFormLibMngImpl.java	1	6a9c9e04b9112b3be64f559da6830215
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java	3	c312d71aa80e90935de87fcad6170099
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	5e4a74e601d83f2f9a41f38724e428d

ms/manager/main/impl/TInsAdviceServiceImpl.java		2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsFormDataMngImpl.java	2	84c83a6da0f51f4625ad5af99b87ea3c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsMaterialInfoMngImpl.java	1	ec0366d1448de5906bb412060db714d7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsMaterialValidMngImpl.java	2	adaae7481e129b9a64e731578156700df
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsWebhallBusinessInfoMngImpl.java	2	1d23d71a6ca18b1f2e1fd6082006a036
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java	1	81eacfdf0c9933da88cdd229433b75d8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TOpinionRecordServiceImpl.java	2	5e3a349f03b76ba5514c7b502fb396e5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TOpinionTopicServiceImpl.java	4	b5df8ce1384bc8136ea14d1cabc7e193
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TQzqdServiceImpl.java	1	9faee0ab34b026022590932d5b2d35be
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TShareClxxMngImpl.java	2	265e42d508a4770a5093bd7f2ff9d5fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java	1	3450e32612b237e9d04c8a2b73941b15
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TShareServiceImpl.java	3	404a12e2fd91b6dc49f10bcfc76881f2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TSpsxPermissionmapsortServiceImp.java	2	013c48d62fa8cb173b037f8f6612e7ea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TSpsxPermissionsortServiceImp.java	2	ba4a82660449119b599f8abfe29a7eaf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TSysFlowlibmapformMngImpl.java	1	83a525a9ac980b367bb01d0826751bb3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallGrsbClxxMngImpl.java	2	d63bd781645131a016f940aa4eb8a845
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallGrsbClxxMngImplgr.java	2	701507395b277fa2fd723450bef50777
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallPostServiceImpl.java	2	a3ab236b4d2aa2cb1cfa3bb38dc33e08
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/VTInsAdviceTJServiceImpl.java	1	18c01462e6874c077dd385046d4f56f3
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	a8a27d3c88485890663bae139817cb

ms/manager/main/impl/VTInsWebhallBusinesTJServiceImpl.java		68
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/VTOpinionRecordServiceImpl.java	2	c738a950a2c17089e500addb249cec67
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/VTOpinionTopicServiceImpl.java	1	ebc66fda04b0af1f7951b8bd8ba1b644
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/VXnjcServiceImp.java	3	cd4438fe908083c9a21058cd45134d17
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebhallBusinessMngImpl.java	3	d61757deaad86b6254574ba84d5c7729
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebHallIncInforMationMngImpl.java	2	f048256965bf0c5529ea1aa211edb053
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebHallUserInforMationMngImpl.java	2	e879bbe3aa3478ab5a8ed7f952d9a2d7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageEnterpriseMngImpl.java	1	78ce0cbda2291b95057a5258a4d6d6e8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java	3	b99ddc3a313966ae4264062dc629e97c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java	3	32ca8f512e2f259bb46f600f71da2b69
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageReminderMngImpl.java	2	14eda8c9713e9648ac3644ef4edec27f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageReminderMngImplgr.java	2	205ccf09df4b04dc7b7e3c9acb696e80
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java	36	69617273f65c65367018190a94b36f83
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/LawGuideMng.java	4	1a92fce92f2b1629a5e028b61e58e60e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/MatterService.java	2	4ba3f916be58b6ff06ec5a41fe206c87
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/PermissionMng.java	3	2527d8878329da546e62492b17a6c628
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ReferComplainMng.java	2	80823585dec2ef6691b87aaaf581cc59
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/RegistrationBureauMng.java	1	63cdff145756d2b1bab8f9fb1dae59a8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/ReservationMng.java	1	82471b09223c7d61123500aad9373d6a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SchedulerMng.java	7	d9209df11c900ff1bb3fe6863eb2565d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SpaceAttachBaseMng.java	2	d16be6ebd423c25e738b28c7c2da670d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SpaceCertInfoMng.java	2	7119d27e4d616cdb91b6c314aa01e6eb

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SpaceClxxInfoMng.java	1	fe9332bb6bfcaf6fc5289724c806a2ed
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SpaceDataExtendMng.java	1	af30558b7d0cd3d500492b2f0427a8ae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SpaceDataExtendValueMng.java	1	2077d400d7ac5c14c2d1925f36d8afe1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SurveyOnlineTagMng.java	1	13eb302ed5bf164e4b70547e876eb9ba
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SyncConfigMng.java	1	63bf0ce9ae0a0de34a490bc51cf98295
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SysDeptMng.java	1	fa4a522f0a6970a99d5ee72f92855233
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/SysRegionMng.java	1	6e5bccb8328e83708a7a5bcbc56a44d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TFormLibMng.java	1	a7e70f7ed53440240412e4750870a47a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/THrUserService.java	1	390ca98d1d885dd2d24a62cea88093a2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsAdviceService.java	1	378cdc3b4f2a5f210be6a9b0821c7fe2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsFormDataMng.java	1	345b911e8898e9af7296a81d6da9197f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsMaterialInfoMng.java	1	e0932e82ecf8581ade96961d6c6ed613
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsMaterialValidMng.java	1	06a289a6a139d3f5955742554a00d302
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsWebhallBusinessInfoMng.java	1	013b00e79449dea1e6eeff51243649ea
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TInsYwpzService.java	1	6c79ab319d991a9a7db57be8e9485ccc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TOpinionRecordService.java	1	96a61b235d71dafa9eec2d2dbfb8adef
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TOpinionTopicService.java	1	93ab0ce76da9628fd0a4b15b366cdf56
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TQzqdService.java	1	f35ca22ca750ac7acc17d1f11384c039
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TShareClxxMng.java	1	77330f88ffb18f4b746681efcd7ddd5d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/tSharePostService.java	1	24155de4eb682830acef94710fdb1508
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TShareService.java	1	6dd23ff50f98d7264fcae13752106be6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TSpsxPermissionmapsortService.java	1	ef8d8d0923a6d6d73675be9d5f1c4df7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TSpsxPermissionsortService.java	1	d0212c3a5bb702d2229905092432f5c5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TSysFlowlibmapformMng.java	1	66a4f728fc3d397f8924307d837529a8
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	0af954d3e3a9fd04e80191a80875b5c

ms/manager/main/TWebhallGrsbClxxMng.java		0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TWebhallGrsbClxxMnggr.java	1	fb14e0f9895367cce5d72027b39ed2c8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/TWebhallPostService.java	1	4a414fe3de0083e88e03610030352683
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/VTInsAdviceTJService.java	1	c44e5dd081a2652718d166b929a3d86b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/VTInsWebhallBusinessTJService.java	1	3b0c97c588c346b53ba867271171bbba
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/VTOpinionRecordService.java	1	39a1fb82bfcb4ab9ee6a2a8722bf2a21
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/VTOpinionTopicService.java	1	6ab947bddebc2d4131575c6e3f212b41
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/VXnjcService.java	1	857f2ddcb15f1bc041a3246a263b9b25
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebhallBusinessMng.java	2	e77e590f63d5158ba6b007fffe41cf34
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebHallIncInforMationMng.java	1	778ee6ed964299cb82a5935922c1b5a4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebHallUserInforMationMng.java	1	ae2667ee75179647a6e7a9a268047166
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebpageEnterpriseMng.java	1	c944bf8772d43caa9c514d55a4d0380d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebpageFavoriteMng.java	2	f5b28ab3a67f6f7d9bebc32dcf5ca717
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebpageFavoriteMnggr.java	2	09363a627c420554f3e5eed6a0d70d6d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebpageReminderMng.java	1	4911c28e0de856624eb65d2737e6055d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WebpageReminderMnggr.java	1	4493548a0b038a71a3eb78abdca2ca06
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/WssbService.java	1	41b6c5faf5a1aeeb0e87f3c25506d3c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java	6	40a3b539b2e46a249e87bf30610309e6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/util/IFileUtil.java	1	9cc4722a50f3cc59cbe639bf18f86dfd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/util/impl/FileUtilImpl.java	1	61a29d0e0b5945b864e267639a7def64
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/Page.java	2	54f637e82a881f3262ebf1fd5dc8b37e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/ReqWS.java	2	570663e136cf9490237cea4f009bc5b8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/Shareinfopage.java	19	1e3277e38862a1433dae38ed75ea119d

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/Constant/constantList.java	2	660b34c47bd20961a33d160771c3c02f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/res/Company.java	4	42ac1002f1133821de6f6b7d8e7f775c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/res/Person.java	3	a26ae3da25e4470f8dae98b7f13bcebc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/res/ReturnVo.java	2	a98f2c806af0995d53b99e68cff2c3b1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/AttachAddVo.java	4	6d91d4641851bcf8d766b0c077176cf8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/AttachBaseVO.java	2	21c60a9bb1e21ca83683a160cb2f1a37
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/AttachBaseVO2.java	3	2c4233f7e1a65a529e3298f809d71d3d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/CertAddVo.java	3	705ef409c7f21327b34dc199c40f2807
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/CertInfoVO.java	3	f6f87a5dc2483f8c5aa6016e4534f34d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/CertInfoVO2.java	3	0a8eec3c0aec2bf839179bed410844b0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/ClxxInfoVo.java	3	b9a876f6440501080ca63aa357f4bf91
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/NewestVer.java	1	45f17b3e80eadb868232fcd7795ec857
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/entity/space/RegSpaceVo.java	3	c9b90faad4a7c1e558bfac39487ce9df
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvc.java	1	3e9b9465095b07f6552fa7e82b3ee561
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java	10	f3746e03f5078c491ed2d4c1d04e7ebd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/ChannelDeleteChecker.java	1	7037f9f7eb643a4b1c82e50105af05fa
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/CmsSiteFlowCache.java	1	29e4353b76e8177fbdcf52ce45ecee53
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/CmsSiteFlowCacheImpl.java	4	8661f1c2055f82970e37ef18f8223f41
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/ContentCountCache.java	1	00dce8aa67d862be5d886350afe07166
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/ContentCountCacheImpl.java	3	2018e48cef1d10600318ff044b343d0c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/ContentListener.java	2	3d5f5104770cce09dc1be3e394ed6395
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/ContentListenerAbstract.java	1	27fdc7445a9cb9a2030872cfa706e70f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/InitSystemListener.java	2	7cfe9d4239134913d1fe6b6eebe8471e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/SessionListener.java	5	b41537b75823d813b9b37178a670b529
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java	15	db6671a097f1c5fa9a1627b0725b932e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/FilePathBean.java	1	f974b527fbd9b05910f4315d8330c816
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/FtpUtil.java	12	b496fa9c9f377d46008d1d7431ae91c1
/WebHallCMSV3.0BAProject/src/com/jeecms/c	9	b54de418039833cea55f6811470b4d

ms/servlet/FtpUtilNew.java		e6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/OpenFileServlet.java	5	4f19acae2c53d1fa2d89d4d6d13dd221
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/SpaceUploadFileServlet.java	17	6526be4e896504c0964bf71a2ebc5e20
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java	20	69be2dc13cc91e5fed9e93103cba3310
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/SessionUtils.java	3	ca17714b8fe88870a22b95c86ad9e4a8
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/SpringGetBeanUtil.java	1	7f29ca4f9129e26b27379497123f9e1d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/ContentStaticPageListener.java	2	9b524d3c161a551d1698dd04070ce2c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/ContentNotCheckedException.java	1	8d882cc37db8670e1924a106de1ece89
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/GeneratedZeroStaticPageException.java	1	c466fae540cf64ab9759590a59aead6b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/StaticPageException.java	1	8bc5991074f2fc79257b65038f64ae0f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/StaticPageNotOpenException.java	1	20fc15cc51dd5fac3d339312e054b8a2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/TemplateNotFoundException.java	1	b053cd942db5fb5fdb8aa6cd40376bb6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/exception/TemplateParseException.java	1	f3c2316c43ce3791ca643405d9a86b45
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticAct.java	5	b7b2a7c57ee8ae766a8366c0a14a2111
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticPageDao.java	2	979f624f8962b27d8979805923a6dcac
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticPageDaoImpl.java	13	151138ca2920a47ddbc000ab67fd8f48
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticPageSvc.java	2	6d04f0fdcf42628d9ac902658a68a0af
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticPageSvcImpl.java	8	d46a84ac6acf41383c4f7c62ec70ed3e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/staticpage/StaticPageUtils.java	2	2f1dadcb0a1c740ba9accca49762712f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatistic.java	4	af40f517b1458a494af5e88abf3122fc
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatisticAct.java	11	64ffc06681cec7be09605b6e4bc152f6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatisticDao.java	2	99b88a91750ce9a55eace554d1cab68a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatisticDaoImpl.java	8	301c3b8f14d48519b23914bdec8d2bf2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatisticSvc.java	1	98d341720e2dfd9a4be746f7c5ae44c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/CmsStatisticSvcImpl.java	18	7d485ae4f79a2c1c5dcf461a4f45ef83

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/statistic/FlowBean.java	2	ef6e4c62b570856105eba81c9ceb0d0c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/StringUtils.java	5	44de21376db4b78ba8b52c7e0eeb0c82
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/SystemConstant.java	14	debfbd45d2f15b0eb3e6e43187c108bb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/TypeFormat.java	5	a8fd7d39976b8500cc21d2bcad149bd5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java	10	37a05f29b3b8d304d99fe720adefa9d2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminLocaleInterceptor.java	2	ba047b54c33b8cbfce41183560bf9998
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsThreadVariable.java	2	e2c16253ecaa5d787ce23d5c5dfb192d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java	2	c1eff2296ebc68999df03911998152a7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontContextInterceptor.java	3	80b94a2612e2e4a7a14e4b8cf304dcdf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontLocaleInterceptor.java	2	4edca02202ac74b0340fe94ef2f88b68
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	15	25388b9eff1700cd828c1fcb13d4170f
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/PermistionDirective.java	3	d94aa74de07989863afe06b785c089f0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/SiteNotFoundException.java	1	f0f9a679f3378fdaf3bb45a2efd55bfb
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/WebErrors.java	2	92f101e09fa4e8ebffdedfc3f3d50493
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/AdvisoryComplainDao.java	1	dc28c3188a27078d5f75a3aae274f7c7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/impl/AdvisoryComplainDaoImpl.java	1	7db90e5889e945e70696ca85a90bc5c2
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/impl/ReservationDaoImpl.java	1	4011c53a2744c3fdb7995e3e9cc8a815
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/impl/WebBusinessDaoImpl.java	1	668dc90543b35eac3908519e0115c9a6
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/ReservationDao.java	1	371848f5a658d910556bbfbc4e1e1276
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/dao/WebBusinessDao.java	1	55e1d2cdbfbf8e94d80fb04c6763a3a9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/AdvisoryComplainService.java	1	1567b15dfa6f59f80c3f819c10d5dedf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/HPService.java	1	515b9269a3c67d6f11e303617b089dae
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/AdvisoryComplainListenner.java	6	60172053afaf4768ef10195fbee2e396
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/AdvisoryComplainServiceImpl.java	3	2c8001d54d1d33b19c114f81e2e34fe1

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/HPServiceImpl.java	9	7bf61e9457ba22bd774b066ba7937dd1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/InstallCert.java	5	4b58d543aecacc80fe87971585cbc4ee
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/MobileServiceImpl.java	4	34428afd826c383e7fddf6e9abbe07bd
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/ReservationListener.java	6	3423802a426d8fc33362d278146df259
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/ReservationServiceImpl.java	3	d3d570de6fac3e094c0bf28fe20fde6a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/SUUMServiceImpl.java	4	048e3c499cd60f00e7eba26b9dc28847
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/SUUMServiceSrvImpl.java	9	2a4de169d2ba9c54c43cfa9ecdda7de7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebAttcheClServiceImpl.java	5	4aea2ee8f41e94868a96d80924aa1487
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebBusinessClientImpl.java	5	1db7807d4398b725936c5061be7eb74a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebBusinessListener.java	16	3b40a5c70b4d7c73da251e3a10755439
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebBusinessListener2.java	14	253bf993b72e79685b7fea52fe3a2a86
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebBusinessServiceImpl.java	16	53bfb8350bf918be5f3fb9f1dfc52f0b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/MobileService.java	1	668b552c9bf7a8fda7e2e1f4f69b823b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/ReservationService.java	1	35a9d14d51d5fa02f0b364d778b30a62
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/SUUMService.java	1	5e458f35bbd10fae0332b0bd3f583c79
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/SUUMServiceSrv.java	1	957cdf567162b0c74f450911f1816be1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/WebAttcheClService.java	1	d978d57d53dbe012eb498b596971dc45
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/WebBusinessClient.java	1	789285c8b4c43451b37406455672f5c0
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/WebBusinessService.java	1	caaa0f9cb6e859e01ae3384c1edadcc9
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/util/Constants.java	1	f0972208fb0ea1a0217af76b7691f2d2
/WebHallCMSV3.0BAProject/src/com/jeecms/c	4	198dbe5585db4baf72c89b092b4890

ms/webservices/util/JaxbTool.java		82
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/util/MD5Process.java	3	3400fa37ca875f1cb55b97fd495145b7
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/util/Path.java	6	d43033945ea40e85a57767128b899057
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/util/PropertiesUtil.java	2	1bf4c931a56486669573a040f87c0c11
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/util/SUUMUtil.java	13	da26533968b0db708ba3aa5a5b45c619
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/Authenticatexml.java	1	99ec6055e67133343d6abd8ac16ade0c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/Businessxml.java	1	95798b37eee8c86803f965ed3ddba67d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/applicantinfo/Applicantinfo.java	2	79dd6a6a491b4d17d9abce7097f4fb1e
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/Busiindex.java	1	dacd9b34878b2929a77c8e2bfe789447
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/business/Business.java	2	d0111f602c26c7b3227b5179954f9601
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/certificate/Certificate.java	1	bc21e6ab270aabbc77478783a27d1f39
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/certificate/Data.java	1	c1f02f159c74744b76584d9c3848300b
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/certificate/File.java	1	be65a83d274056e925eee1a64513e60a
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/certificate/Head.java	2	896ec9eb2419882d60b45b16bd115348
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/certificate/Nodes.java	1	02c2a7247d024b8ca998b7869082f912
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/chargeinfo/Chargeinfo.java	2	904007fe05d3b55717b33cc2f3bdf1bf
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/chargeinfo/Chargeitem.java	1	111775cf814437ec6b485db815307ff1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/form/Form.java	1	e18ee392c5b6978bf50e2849592ad499
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/form/Forms.java	1	262423edac1113c7b20c4ec4898bf510
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/material/File.java	1	d90ac11e50656a53d3b0419bf278455d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/material/Materialinfo.java	2	7014cdb4f8bf3835009dcd84dced717d

/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/material/Materials.java	1	9cd78151e53830ee34b9c989fff5bc89
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Acceptnode.java	1	689b1ca0e7b40a9eee1f26032583e5b5
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Applynode.java	2	1ac754b595084e608e67f39210f71175
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Complementnode.java	1	0852dbc4869ae67e5d74506fe5d1450d
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Handlenode.java	1	a16e29bf89654b35deb82210ca59c5ca
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Node.java	2	db7496f6344a3b55d54d9d981889d458
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Notifynode.java	1	acc9010b9c73c729b4f19bd7d7a533ab
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Risk.java	1	a09057caa1c4ffd52f3b100e0cc332b4
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/node/Specialnode.java	1	094f15e0e29149d5080e4128872044d3
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/Permission.java	3	9630b11d39263fc92f93a87e37d67985
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/cooperation/Returnxml.java	1	95b2a7b6494603a626db2d8d6ff200c1
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/Refercomplainxml.java	1	9c9dcc95eb7beb1a650c108f95fc173c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/Reservationxml.java	1	b6b94f164ce8c84604e036383f364265
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/vo/WSBean.java	1	078dce5b55b122bb6006b7efe9c7080c
/WebHallCMSV3.0BAProject/src/com/jeecms/cms/WebYWLSHServiceImpl.java	4	bf0b7f8375ab314123636e51329a4648
/WebHallCMSV3.0BAProject/src/com/jeecms/common/captcha/JcaptchaServlet.java	4	8fd3131f240e2ccae1022c640487c534
/WebHallCMSV3.0BAProject/src/com/jeecms/common/constant/NumberConstant.java	1	f29f344285ff6e951f94e854ebd96c8d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/constant/StringConstant.java	1	23c88db48f458f1fda435c53bf183f31
/WebHallCMSV3.0BAProject/src/com/jeecms/common/constant/WebHallConstant.java	1	0eeefca4ccd2f1c49ad7cbd934ca4916
/WebHallCMSV3.0BAProject/src/com/jeecms/common/email/EmailSender.java	1	a39c7f80da8613b2303ad622de1bb85c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/email/MessageTemplate.java	1	0bf2043906b25c08770f961340247866
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/AbstractFckAct.java	1	1a3adc701a11a703b9ae0a5f91543c2a

/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/Command.java	6	4b16f19cf56895f9a2fc196a1ec1cf3c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/default.properties	1	5b3fc29e63f05a5a8dff744cc4825a87
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/LocalizedMessages.java	7	e45019a099fb540cb9f8961ba60b0da9
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/PropertiesLoader.java	6	68f186216f9919e156303c03ae226f80
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/ResourceType.java	10	d64d55dd393012f4fae145981e6d79d0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/UploadResponse.java	7	54f970bdfedbc340d8774ae6d64a971c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/Utils.java	4	17bfa7bdfdaa1caa81be20b9807996d9
/WebHallCMSV3.0BAProject/src/com/jeecms/common/fck/WriteException.java	1	4bd46cc92e539f3f8d3f00dcad7fce54
/WebHallCMSV3.0BAProject/src/com/jeecms/common/file/FileNameUtils.java	2	8bfbcc4e53a6eaf0faff1ff98c51c3f7
/WebHallCMSV3.0BAProject/src/com/jeecms/common/file/FileWrap.java	6	e1c8da5b450e86c96e2665a14d4c59d0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java	8	1c40a0f9af6c9bc0f0e1eecc26ffd230
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	6	d66ae32f0a3d6d71e3f620186651b092
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	6	9cf92380c7ccdebc650f1817f8bb9ca5
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateTree.java	2	35de2a31bca80fbb71d14fb55d0fd505
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/PriorityComparator.java	1	feb32526a04cc3a081fdefaf93ec2610
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/PriorityInterface.java	1	484004582d5f2ce148cd370176460171
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/SpringEhCacheProvider.java	4	752a39cad10b9d4106b0310c1f7982e9
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/SQLServer2008Dialect.java	1	a46707f54a497d73d135dda00a8c7af8
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/TreeIntercptor.java	11	7d5f707c5446276da8534c20ce69a6a4
/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Updater.java	3	69b8a1ef4e9200a165d0a33300861003
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/AverageImageScale.java	10	e3e72d4396a5de79322ca8198402aefc
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageInfo.java	36	ca5344e7e69f27ad106c1e3d6953a3c1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageScale.java	2	08699c31491ef8d45beaa0ee5eeb9b58
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageScaleImpl.java	3	a1e4df0fbf0ee1d63e04a1c349262af8
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageUtils.java	3	4bab3dcedf16e143e22e2726445a8267
/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/MagickImageScale.java	7	80f429282395d13ff22e4383a279daae
/WebHallCMSV3.0BAProject/src/com/jeecms/c	1	effdf0552b5a4b4c43156629082bdc3

ommon/ipseek/IPLocation.java		d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ipseek/IPParseException.java	1	fefe4f0e7d86bac42bb2af5073ea4f22
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ipseek/IPSeeker.java	1	847af9987f8377fe8646b76b066e68c1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ipseek/IPSeekerImpl.java	11	b90eefc5c77e51778e223cd1e1a8b590
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ipseek/Message.java	1	6a022eca3d03501283bf6a41cfd2cf2d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ipseek/Util.java	2	ae2832e7dbcac5b11ea7ac065ef21382
/WebHallCMSV3.0BAProject/src/com/jeecms/common/lucene/MoneyTools.java	1	b07cd87a44e6c02b742a915abf86f2f0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/page/Paginable.java	1	69d41ce1162e3c56585c449a2ac22ffe
/WebHallCMSV3.0BAProject/src/com/jeecms/common/page/Pagination.java	2	14c8e84ab52027e3ce2d7d818dab8676
/WebHallCMSV3.0BAProject/src/com/jeecms/common/page/SimplePage.java	3	caead2a1b37c94afef5ca424405bd9ec
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/AccountExpiredException.java	1	e7b2d6b0c466976a6915a1324e271c69
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/AccountStatusException.java	1	622e074533adfbb220dbad34bc51e407
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/annotation/Secured.java	1	3c39db02b5904064678534433fe1f25d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/AuthenticationException.java	1	de208bc94e4a0d9d13d830a4db0ec761
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/BadCredentialsException.java	1	a97cee8907d8600e54821f2ac1b09f2d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/CredentialsExpiredException.java	1	ba7f9d8e5aa9c76799f737a2afbc1c58
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/DisabledException.java	1	046d13141c68d4dced0cff790d00dabc
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	3	11fb2017640d4d311197ffbcb2aa3a3b
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/PwdEncoder.java	2	42c666b405b9bc84176002c1870668b9
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/LockedException.java	1	12c561dc6306a83a40a6668a2388a50d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/AbstractRememberMeServices.java	12	550eeb20743e35b37c2b306082ae49f8
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/CookieTheftException.java	1	fc5e19efd1273e2d4f35f0f7c4458a66
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/InvalidCookieException.java	1	2934ae285af2e378822076603c3a519e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/RememberMeAuthenticationException.java	1	6602374c9996d50ec4012d1953128440

/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/RememberMeService.java	4	d868a4d539bd52502a822b4f1716defc
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/rememberme/TokenBasedRememberMeServices.java	9	60de9c337a273db934d448da76e1493e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/userdetails/AccountStatusUserDetailsChecker.java	2	1cf43a8931d50f6c001f8f8e8b9b6ed9
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/userdetails/UserDetails.java	3	c0d64c40bfa7dcfac890e9ff624e02a2
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/userdetails/UserDetailsChecker.java	2	540222273adb0cf908cdcdeee958fcae
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/userdetails/UserDetailsService.java	2	fa8ae8d490ae17bbd60831ab378bbd2b
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/UsernameLockedException.java	1	869d7b3cef509e64012f8acae3ec179f
/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/UsernameNotFoundException.java	1	b6b54d9e8e3a20137152d51aa6a9a0dd
/WebHallCMSV3.0BAProject/src/com/jeecms/common/sm/SendMessage.java	9	c99c8fb8e450b3ef245a4d22e4ad75f5
/WebHallCMSV3.0BAProject/src/com/jeecms/common/sm/smsendsql.xml	4	b27cfba8b2a947f6a02aec64040a759a
/WebHallCMSV3.0BAProject/src/com/jeecms/common/ueditor/ActionEnter.java	4	47882e9d96b6550c991b0c823827b375
/WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/FileRepository.java	3	b47dad1e7bd6909da59534cd57d5c900
/WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/MongoFile.java	4	6e998fe4154874416eaa486b2192c491
/WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/MongoFileQzqd.java	4	e2e4e1e3bb4eb0b4eeb2394eb035811a
/WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/Repository.java	1	fc9621f64e9b8c96f5dea292c04be6db
/WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/UploadUtils.java	5	3d85c4ba01118e88c4be499a8666d489
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/AESEncryption.java	4	e56d241ee3abb3d7fdad826475198177
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/ArithmeticUtils.java	1	ae57d8d44a5b295562284496c6deb3da
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/DateFormatUtils.java	1	6f0828dcc3ba784d2c87358255635925
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/DB2Test.java	1	bcfb5a1e4aaa805e69467ff2917d063c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/File.java	8	db832f63c620b3d19f6553e227d5de8c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/Files.java	2	a6990c7543c51a0e75a94e636d8666f3
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/Request.java	2	8163bbac38cec4cd90a5cce57e311ec6
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/SmartUpload.jav	28	95f59e734a7054506283fb3c8bdfa4c0

a		
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/SmartUploadException.java	1	ca265228aefb375675d844dfa9e0796e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/mail/MailSenderInfo.java	3	d5239e1179c8bd960512f76ef808c242
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/mail/MyAuthenticator.java	1	3d658cd8a05803bcc2040f2e0b2c7e97
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/mail/SimpleMailSender.java	6	a021259307e13d78ed6127a761cbe3af
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/MyBeanUtils.java	3	53b5e7d550972b345f6388e3f0841cd1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Num62.java	4	363694d1846c497bd1160a0624ebbc2c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/ParseURLKeyword.java	3	bfb9eba00fe4055224c2c2426403fc2e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/StrUtils.java	5	272417a53091d05389194a07cabeddf
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/XmlUtils.java	2	eda9c16b4bee2d570bf283f73f01ff10
/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java	5	4c8250560dd5c3cf6ffd50dcdd4f9280
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/Constants.java	1	b41ee722cda6c9e555774ef2f6479f35
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/CookieUtils.java	3	00b239a8c05d4a840aa6992c1ae86a4c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/BufferedServletInputStream.java	6	3d8c4b112855a1099e979b1f78004072
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/CosMultipartHttpServletRequest.java	6	f2c7b8bae12a34c0efaba346fcafc2e2
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/CosMultipartRequest.java	19	bf490f7528fec4130f5295d47ce3a29f
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/CosMultipartResolver.java	9	19f5e998a62c76f4a3ed6e8653bf859d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/FilePart.java	7	4400dcc90d37ff4267536cc6743cc919
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/FileRenamePolicy.java	1	aa6ee5dd94274526215d407f546278d0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/LimitedServletInputStream.java	4	2335d5ce3115522647bbf0b5c710cce1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/MacBinaryDecoderOutputStream.java	2	e2e2f9dbfd1f09395048a73d420d10ef
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/MultipartParser.java	18	9edbd2a9eaa43faeef46f5c5c6b8ca01
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/ParamPart.java	3	606b16abf88ef765ea9ced6982255759
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/Part.java	2	08f7ad2af30e95c958b4e78d0348ed3f
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/cos/PartInputStream.java	8	c8bed27d30ea6ea0cfac9e945016f3e9
/WebHallCMSV3.0BAProject/src/com/jeecms/c	8	4206105ce303844499fb26d1f0ae500

ommon/web/freemarker/DirectiveUtils.java		d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/HtmlCutDirective.java	2	0cb0c379863dabeec96279e795483de1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/MustBooleanException.java	1	fbc429908439f81a3233e8952fc6b628
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/MustDateException.java	1	8a37ceea4e4cf9a5e43b224ed4cc80e0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/MustNumberException.java	1	fad90f1c188fa4c96278ca7c9dc775b3
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/MustSplitNumberException.java	1	3f90bca9f0b679438ca16bd7a824c67e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/MustStringException.java	1	51ef21c36b78b3b9a6caa1f5010a4969
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/ParamsRequiredException.java	1	ec54978b96d0c6145de2c6004ef3f4be
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/ProcessTimeDirective.java	2	783ba8984e259192d418948d5891e3e0
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/TextCutDirective.java	2	e1135f4581857d8feab6f8cc4a60f8d4
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/freemarker/UUIDDirective.java	1	69db28e9fb142503a01f141bc02ac66d
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ProcessTimeFilter.java	2	b644ab6f061f92cbd86b71e39dafdeb7
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	8	7b0a4570631e527a37e0c980fc241c17
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java	2	adb13fa14db3402793aaa4b8342b4bec
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/cache/EhcacheSessionCache.java	2	f73f01598d246d5cad6ddd6f7aad8687
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/cache/MemcachedDangaCache.java	3	aecbcd00dac0261e9a4f45ac0214d37c
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/cache/MemcachedSpyCache.java	3	4ce5bbd666b45ff8e3c18c1ba9e3acc2
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/cache/SessionCache.java	1	c782b509843193195ebbfdf08a3a3d92
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/CacheSessionProvider.java	5	c2380504392d8a877098ea6aab65a9a1
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/HttpSessionProvider.java	2	0d08cf852b4b1d683826cdca955f80ad
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/id/JdkUUIDGenerator.java	1	e058d14a835abf2de73744d3a8f7abe9

/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/id/JugUUIDGenerator.java	1	2cb4edfa4b17aeb3e58f79569bb7a272
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/id/SessionIdGenerator.java	1	3350c689cff8edcf56a7ceca0819b5e7
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/session/SessionProvider.java	1	3f385f0a10c8d0d63f0f12643522d3ae
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/BindingInitializer.java	1	2dccfafdcb0a5d1e1419a43177f72cdf
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/DateTypeEditor.java	2	ecc8b3e6082b3549464c0520651cd6b5
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/MessageResolver.java	2	66f554ce01069992b1e1720ccc27ed44
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/RealPathResolver.java	1	ed8eef5d7acf8a5f8988268d288b1737
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/RichFreeMarkerView.java	1	f3b1e8bc4e982e5dba33f7bdbf4ccc55
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/RichFreeMarkerViewResolver.java	1	5da8eb9eec3a400e10a1ad3841e25544
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/ServletContextRealPathResolver.java	1	e33ee12fa9d027b8d2d1f1aab22f8e7b
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/SimpleFreeMarkerView.java	4	9cf8b68db941492ed7477b3b50d96f5e
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/SimpleFreeMarkerViewResolver.java	1	3d8f28f7ce80bbf87a944c2fac60e2a2
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/WebErrors.java	7	59021a9307193a8269fe4d547f7a608b
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/WebDirective.java	1	45fb047ec95e45561dbbae9f5e389353
/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/WebEhCacheManagerFacotryBean.java	4	757404516bc7b6bcc2245dbeabc229ab
/WebHallCMSV3.0BAProject/src/com/jeecms/core/action/front/DbFileServlet.java	2	c09a9c05546ae6fe5c2d8ff4c319d2fc
/WebHallCMSV3.0BAProject/src/com/jeecms/core/action/front/LoginAct.java	8	c598223a4512693c4b837a6ef8a817f0
/WebHallCMSV3.0BAProject/src/com/jeecms/core/action/front/ProcessAct.java	2	c1abe0b88d2dc07ffeeb1352c92f87f1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/Constants.java	1	ce79e9ecace4686f7d3484bcdeea8d70
/WebHallCMSV3.0BAProject/src/com/jeecms/core/CoreException.java	1	c1564098b31daf4ef4d385e8832fc9bc
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/AuthenticationDao.java	1	5e40f5133eb523937f6a229cb104b786
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/ConfigDao.java	1	b2ce0615e72c873cbceae6af114850bc
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/DbFileDao.java	1	c496f6bf2e0cc34dd4a3f817306a6064

/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/DbTplDao.java	1	0ca5ba7191a537dd343f164f00cddf79
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/FtpDao.java	1	558500058909695647b622aea31ff8de
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/AuthenticationDaoImpl.java	2	4ad6e850e28ea3ccce7bb22d97db52de
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/ConfigDaoImpl.java	1	1feec6f35f310c32dfb3f9d239cdbe46
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/DbFileDaoImpl.java	1	b634cbcc4a31471aaff7fa9cd2dad9b4
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/DbTplDaoImpl.java	2	0acf2846c96970a8278472636fb3fa86
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/FtpDaoImpl.java	1	b8ba02a5ee2614ff0cda6438f90d889b
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/UnifiedUserDaoImpl.java	9	c5d6af0842d3ca94212ef3d47234505a
/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/UnifiedUserDao.java	2	f664fd94a89c7474c879eba52b0492a1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/Authentication.java	1	122f1dc344ede67bb24643a4518ab060
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseAuthentication.java	5	1c66401913adc12d618d7f248941ab51
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseConfig.java	3	882836f1a7bb1f0b6abaf19d4fa78479
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseDbFile.java	4	c347dbd98edd70d842febec9e8c4ff0f
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseDbTpl.java	4	c37003ebfa7298b408f9fd3cdd2ad080
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseFtp.java	6	ed8e7391abe8b211fcdf5606b651e7a8
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java	11	05d6e007974088e49001a79417af9596
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/Config.java	7	3405be05e33e00268b1f73ae9e06d04f
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/DbFile.java	1	31e25993887849f39a21d68f0047f1fb
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/DbTpl.java	3	05502bbf8b499ceadb05113242a79e30
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/Ftp.java	4	9cb6479d6891cf7244959b26c2631e31
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/Ftp.hbm.xml	2	eb45eefc033c2f8a1e179084cfac96b0
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_db2/UnifiedUser.hbm.xml	2	2825d95047e765324fc57ace529de209
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21

/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/Ftp.hbm.xml	2	ea2a9737ba407230eeda61969956bd6e
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_oracle/UnifiedUser.hbm.xml	3	3eaee0a998b87db5885218abbe072785
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/Ftp.hbm.xml	2	eb45eefc033c2f8a1e179084cfac96b0
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/hbm_sqlserver/UnifiedUser.hbm.xml	2	2825d95047e765324fc57ace529de209
/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/UnifiedUser.java	2	a09f37fbe241971efc685b2e2b0465b5
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/AuthenticationMng.java	4	f9411c9becc2452b3873535158869eca
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/ConfigMng.java	1	be481f05a4631f87ed0cb23a8ec74028
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/DbFileMng.java	1	4b39c68f3f40ce5d5137f77fbb0340f2
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/FtpMng.java	1	d09b79b5bd686b15aa84834c75f05920
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/AuthenticationMngImpl.java	7	a39518f04bc624c96e2c5fd42f6979f1
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/ConfigMngImpl.java	3	f4a1903a2de9e421d0c262ff0e573d09
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/DbFileMngImpl.java	3	260505bb712dfaf7dab5c95262901e80
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/DbTplMngImpl.java	6	85b626955c9beadd6fbdb18818e53fc6
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/FtpMngImpl.java	2	9f7c31b17c2441ca29f6d38f10cb2eda
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java	14	28c3b720a9620d48accf442eb60d7791
/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/UnifiedUserMng.java	4	4ca6d5c9393d5ce1a2cc062a989aee39
/WebHallCMSV3.0BAProject/src/com/jeecms/core/tpl/FileTpl.java	2	3db50a47159f1e124647d65b927ac459
/WebHallCMSV3.0BAProject/src/com/jeecms/core/tpl/FileTplManagerImpl.java	5	ceb620febe2892a0e784f5b68186c757
/WebHallCMSV3.0BAProject/src/com/jeecms/core/tpl/ParentDirIsFileExceptioin.java	1	7cab3d2b52d836186db29b9bc517c8cf

/WebHallCMSV3.0BAProject/src/com/jeecms/core/tpl/Tpl.java	1	0463edd00524d7cee1577130969b62cb
/WebHallCMSV3.0BAProject/src/com/jeecms/core/tpl/TplManager.java	2	fbcd40512cc74cffdf8634cee125472d
/WebHallCMSV3.0BAProject/src/com/jeecms/core/web/ContentInterface.java	2	6f682e7385548a5d34b2ef6bce88cd6e
/WebHallCMSV3.0BAProject/src/com/jeecms/core/web/CoreUtils.java	2	316e3e76ae72f11c6305b364bf07e8e8
/WebHallCMSV3.0BAProject/src/com/jeecms/core/web/front/URLHelper.java	7	bb31d63114ecf3e53c233ec3a29bb15f
/WebHallCMSV3.0BAProject/src/com/jeecms/core/web/WebErrors.java	2	56476fcad5c2ed6b9dc4616200bd1b5b
/WebHallCMSV3.0BAProject/src/com/tjsoft/module/synchronization/model/Sync.java	1	1fe4f736a41a00fa74468fb20f165756
/WebHallCMSV3.0BAProject/src/com/tjsoft/module/synchronization/service/BaseDataSynchronizationService.java	1	206114e3d4d215173d7e0be5a80fe1a3
/WebHallCMSV3.0BAProject/src/com/tjsoft/module/synchronization/service/impl/BaseDataSynchronizationServiceImpl.java	14	f47b01904ce7321cb9902fbff9ee8a86
/WebHallCMSV3.0BAProject/src/com/tjsoft/module/synchronization/SyncType.java	1	7e062ddb1dd62d56d19f43d3b3cfee18
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/common/util/Constants.java	5	e98743d5dee92fadf8c0570f7970ad1a
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/util/DateUtil.java	5	d43912472f9c562a043a644a9e0dcf92
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/util/SearchModel.java	2	fc793cb3bfecf766a6eef95396c3ad99
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/util/SearchUtil.java	4	f7616ae3a49f4696ff28131d92378dba
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/util/StringUtil.java	1	1aa12dd2294254abbb90b12b6e2f4c66
/WebHallCMSV3.0BAProject/src/com/tjsoft/platform/util/we.java	10	1820f2da995b1534625cfd7519db14c7
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/Constant.java	1	717c0fafd5de0899564bf8c8871371a9
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/dao/QuartzDao.java	3	8ec6531decc42c8e5a71875c7c98bece
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/example/MyQuartzJobBean.java	1	1555738a555a5d571ffedde945831090
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/example/SimpleService.java	1	9d6875a0b55c33a4d0b16be08feb4801
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/jobbean/IQuartzJobBean.java	3	7d997127d57609c4fa2ba0b8a7234886
/WebHallCMSV3.0BAProject/src/com/tjsoft/quartz/jobbean/QuartzSpringContext.java	1	7b168ae8849670ef46ff7a87993f87c4
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysDept.java	8	8932eae3eec0eeb1c4614088910a9142
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysMenu.java	7	5a68cad40f755448137e6e1da34a9c36
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysRegion.java	3	34ad2e42dce0432070009f4add8510c1
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysRole.java	6	9347b4df6fcf2e1253a6d3da4c04db9d
/WebHallCMSV3.0BAProject/src/com/tjsoft/sy	4	1444987cf853f2cd0519d340d18c64f

stem/model/SysRolePowerMenuAss.java		e
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysUser.java	11	16cee3c764973f02be89026e02afab0f
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/SysUserRoleAss.java	3	e6a3aa6d0b26076207a48c8cda72987a
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysDept.hbm.xml	3	a405199cb59dd9df6483d1dcc7420b26
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysMenu.hbm.xml	3	cbffcac05fe81bff23c4da23e0a88c8f
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysRegion.hbm.xml	3	57b9199f30869089d82672bb166af4b5
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysRole.hbm.xml	3	9089730308b816d47294b63b57d250c7
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysRolepowermenu.hbm.xml	1	76d478c2999e98e9a8c2a7963cd4b2cf
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysUser.hbm.xml	5	6a3401f91dcc8b42d8618029b62c1bb3
/WebHallCMSV3.0BAProject/src/com/tjsoft/system/model/TSysUserroleass.hbm.xml	1	4b2dad5ec9c738f04676d1cfb5a6a0b1
/WebHallCMSV3.0BAProject/src/com/tjsoft/unit/scanningByPhone.java	1	73d208421447f99ea43e3e79d0dd0d9b
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/client/MainClass.java	7	3daa465126931fd06552c0720ef3801e
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/client/Test.java	3	05848eeb26cc910ece7ef3cb86fd12c7
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/client/TestService.java	3	f92089d1d914f1887c1a1dab535a1fd7
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/DataServiceFaultException.java	2	d950fc1db4f09f35be88ce75d7b1a435
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesCallbackHandler.java	13	68520e2dcd7b3c238c6c1406601a0d32
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesClient.java	12	ce75bb3b27df3ab54280c2c2756206d2
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesExt1CallbackHandler.java	4	3a988412b6b0a648677807b129d8ef3a
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesExt1Client.java	4	0ec86dd5dc104607dd473329db63e648
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesExt1Stub.java	300	8a62e0abff8bb8266e27d31e1f609d43
/WebHallCMSV3.0BAProject/src/com/tyky/cmashup/services/stub/PlatformBaseServicesStub.java	1,760	aa1fda2f1a90fe87700feef53dcd9946
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/filter/CASFilter.java	15	418dc3852b89a2ba062b8b6ca26a0726
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/filter/CASFilterRequestWrapper.java	3	de03478001330e417b5c453529d0c0a3
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/filter/InjectFilter.java	6	46e26dc6e261e8e3d43f5a04b4005e23

/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/filter/SimpleCASAuthorizationFilter.java	4	f328db744c269197fc1e01b262715a52
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/ProxyTicketValidator.java	6	8e8077f59bb3f4c8e768e386bbf30884
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/ServiceTicketValidator.java	10	b307467af734b030a224af83e010f5e7
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/AuthorizedProxyTag.java	3	80fe8f3efe0916505861dab6176ff74c
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/AuthTag.java	8	8fec54ec4ae7291de78adbef7ff3d78a
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/LoginUrlTag.java	3	0727a5392a67e254e60d1aeb37937b1b
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/LogoutTag.java	5	a4582e3ff12eae00a09a9282fe520a68
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/ServiceTag.java	3	72f5374fbc93cd15ea0cfd00bca26476
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/taglib/ValidateUrlTag.java	3	0612da73a08e26a2d5e05bc0b3e9d7ed
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/client/Util.java	8	b04e9b70f49d485a3b0ee5d5814180f8
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/proxy/ProxyTicketReceptor.java	5	31c86f975760523b7567979999b088b8
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/util/FileUtil.java	2	ae0aa743ce603782cd771b46e2b9e030
/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/util/SecureURL.java	4	379d851568ae5e22849d946dffeb8158
/WebHallCMSV3.0BAProject/src/ehcache-application.xml	1	619d7af435973fd88bea58bfa29294a1
/WebHallCMSV3.0BAProject/src/ehcache-hibernate.xml	10	20f797e7dfe0a5418e455690466e28a2
/WebHallCMSV3.0BAProject/src/fckeditor.properties	1	56fbc690b28bbc53f4433c3aee205ab6
/WebHallCMSV3.0BAProject/src/logback.xml	1	e1fac0da7e0251f1a8be9168b5723f74
/WebHallCMSV3.0BAProject/src/quartz.properties	2	5ea29b24af40ee970e6d8319236eecc1
/WebHallCMSV3.0BAProject/src/Service.properties	2	571b019743ac49f8ba56d2d6b07fa221
/WebHallCMSV3.0BAProject/src/sms.properties	1	cf9683f27c598c38112bd3ae71f07aef
/WebHallCMSV3.0BAProject/src/smsendsql.xml	2	320c489b079a60f58a4032e35ba5c84c
/WebHallCMSV3.0BAProject/src/sso/filter/SsoFilter.java	2	3ae2332ac47ade3554b3b62ead12e6cf
/WebHallCMSV3.0BAProject/src/sso/test/test.java	2	847fecfed77488234c1e7c5c641d4f37
/WebHallCMSV3.0BAProject/src/sso/utils/SsoUtil.java	4	4178057ba68627d3b80b0e5fb8009d51
/WebHallCMSV3.0BAProject/WebRoot/404.html	2	cd6415ec10535808fd0e9f3c8ec8ff2b
/WebHallCMSV3.0BAProject/WebRoot/500.html	2	506768386c3c4fabf36aa593dfdb9939
/WebHallCMSV3.0BAProject/WebRoot/error.html	2	488c64051295d45621ead7eb525cbaa6

/WebHallCMSV3.0BAProject/WebRoot/foreign/bottom.html	4	6babff6233c2a253052ae0b509396e96
/WebHallCMSV3.0BAProject/WebRoot/foreign/top.html	8	e7288e7e23dc835aaa93e68ab7ebf108
/WebHallCMSV3.0BAProject/WebRoot/home/findCommunity.html	2	c930334961b2b303f65d47cad7d0df2b
/WebHallCMSV3.0BAProject/WebRoot/META-INF/MANIFEST.MF	1	d0e895251c05b9ea895dda3a15b060db
/WebHallCMSV3.0BAProject/WebRoot/MyHtml.html	1	918c8ca74f291072fa4bc56bad67e2c1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/ajaxupload.js	26	61108dddf6f3de382f8e4612c12b674c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/AsyncBox.v1.4.js	12	22906bb72f42a98f1bb00a7b155246bc
/WebHallCMSV3.0BAProject/WebRoot/r/cms/bid_bjca.js	12	9fc591defe9773406ce192235b5766ca
/WebHallCMSV3.0BAProject/WebRoot/r/cms/captcha.js	3	a5d55f64d918b106aa0806ded22efb25
/WebHallCMSV3.0BAProject/WebRoot/r/cms/commontools.js	2	ed49eb5dc588ffe778ba84daaba30fca
/WebHallCMSV3.0BAProject/WebRoot/r/cms/formTool.js	1	9db8d5d05f4431df0b32853ab5a84974
/WebHallCMSV3.0BAProject/WebRoot/r/cms/formUtils.js	6	aee037fe4b55d6c10d879352768e9cc1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/front.js	6	76196ddb67c272f2664d235524a7e541
/WebHallCMSV3.0BAProject/WebRoot/r/cms/htmlFormPlus.js	3	42bac0b773a2840ac46f4901a7804cd6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/jquery.hoveraccordion.min.js	6	65c9b445561bfdc831b366fe22de74f2
/WebHallCMSV3.0BAProject/WebRoot/r/cms/jquery.js	193	00a7c34c360eae65d1096d97a07ca24a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/jquery.qrcode.js	3	fa248c8d93963355e7a897aa188396ef
/WebHallCMSV3.0BAProject/WebRoot/r/cms/jquery.qrcode.min.js	24	4a9ed555c31d4a2dca088ac0824d1410
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matter.js	30	fd8cf4c1fecaed1cd6cb74971f7d10f9
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterdetail.js	32	0786c06685057d7ec899d6238d322191
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matteredit.js	39	9f407d10c70d9bd3da7d6e53a3a38501
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtml.js	60	421d9a7157760f2ea4c1d5f75f78ceee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmledit.js	65	d4619e727d995e80642ae190d85a5e42
/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js	62	f5d7030e873b2be17ba417c272542d24
/WebHallCMSV3.0BAProject/WebRoot/r/cms/ocx_bjca.js	40	c120e39616374bbcda35a530619347d1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/popUpManager.js	13	61c48712a4a999c08efef1678b9d7489
/WebHallCMSV3.0BAProject/WebRoot/r/cms/qrcode.js	36	aef954d4039be1b2f65a5bd2fb337df0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/si	3	65dad8feed1eb2f9bbd7d3087b225cc

mpleMove.js		a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/tipswindown.js	7	cf6addf8adf8160f435b16b69e363590
/WebHallCMSV3.0BAProject/WebRoot/r/cms/validateAddMethod.js	9	5706db4a5045cf18f4a8c922d2181904
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/cj/Scripts/swfobject_modified.js	22	6b21d8c2c636c037a41c9417e40050ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/index.js	1	9b16fb1c5eb8c5c8233f31c07bd1d0e1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/jquery.autocomplete.js	21	11e6e59dc34688d98c5c9124065c244b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/jquery.js	98	b89bc081e965c30dbc7ff2cedaed86e1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/jquery-1.9.1.js	263	b14c1226d284c67612f3a672ae4aaa8c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/jquery-ui.js	577	d09e56bd109775783828a4f6f7a69c31
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/localdata.js	1	c4f22e733863ac7fb499cc92703f0377
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprise/js/lrtk.js	1	a6200ee7bc54bd39274e0cfb95472570
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/index.js	1	9b16fb1c5eb8c5c8233f31c07bd1d0e1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/jquery.autocomplete.js	21	11e6e59dc34688d98c5c9124065c244b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/jquery.js	98	b89bc081e965c30dbc7ff2cedaed86e1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/jquery-1.9.1.js	263	b14c1226d284c67612f3a672ae4aaa8c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/jquery-ui.js	577	d09e56bd109775783828a4f6f7a69c31
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/localdata.js	1	c4f22e733863ac7fb499cc92703f0377
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/enterprisegr/js/lrtk.js	1	a6200ee7bc54bd39274e0cfb95472570
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/common.js	1	bcbbed23ee7018ae1ef7fb91243ffe56
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/heiphoto.js	40	8058f0e0b741c7fd14992261a6b8f8ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/message.js	4	f08530cb346e45d3941fc819b14f4363
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/p-cr.js	57	d957933ea645c85687be1b3c9ecd8883
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/p-cr1.js	56	67fb4458711f487f9ffc88bd497ce6ee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/js/sinaflash.js	7	3a1ff60f956d80dc9f4cda3611bf754d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/	1	0906723e6df6db37d3b4cc64d70138

www/blue_webhall/js/tab.js		14
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/mobile/js/ajaxupload.js	26	67b5d9448287f9e402c835b74a6067f3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/mobile/js/jquery.js	133	3a8a2df9830678982955a463e5a722ff
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/mobile/js/mobiletools.js	4	786a7ff3a4b06f6fae19fd1a349b1234
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/mobile/js/swiper.min.js	112	ada6f0aefb6a409b94380f5fa4a20bd3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/index.html	1	2ccd8a4a9ee6faca2ada3c63a0782fa5
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/left.html	7	0138e7c97cb46b0c36e1ce68ab8db1b0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/main.html	2	b6c86b8f3749c5246d5b6ac1e939bfc0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-a.html	2	a5e29f5cc8e9636f02d0dbe1d3b35a48
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-b.html	1	b4cddac58dc86e5d3ae35f60867203f7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-c.html	1	166d88435e907158c1d2799b08338fc7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-d.html	1	bce62a9fd29a3cd799ce9bb26bc5cc6c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-e.html	2	49cacc2cd3db44c6c8e4110280a14fed
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-f.html	3	8a6f2644c0c85214908b5c2310e24990
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g1.html	3	e7994ec29fae4e276277ee64baa016ce
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g10.html	3	01934ec4eb68be39150b16bb8a366986
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g11.html	3	46f781fe73b71b99f337dd52efd58795
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g2.html	3	42fd7a8cbe0e0b1c406c767a676374fd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g3.html	2	3cfaab7361da2176b4d501378d5132bb
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g4.html	2	7d1916e684089cc0ad59f7fe3326942a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g5.html	2	8a3b609bc1e50a9ecd31d9c01c65a718
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g6.html	2	d136beb653fd9ad947decfd34ebf6315
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g7.html	3	a3e787f5b6881417614ebe018f27a68f
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g8.html	3	f0ee8233ba038d6f8d073b39fb0c477c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-g9.html	3	d2418369b0b96af2534209d1cbd0c658
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h1.html	1	44d01c7aecb4a51eb28a88c5d77dcb47
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h2.html	1	88a5956c82b892ee36a30abfd6761abd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h3.html	1	3ef91e6ec2d5ef0259eab39c1462457e

/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h4.html	1	df1fa27d402d69cd051d38bff111d663
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h5.html	1	3fe01dbb7ca6a0ac5ee98171f39083ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/right-h6.html	2	b6d47e61d8420515d21fabdf45c55f84
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/navigation/top.html	1	cd783f270574a9aa1285ceac9deaef0e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/new/js/jquery-1.4.2.js	161	c0ac4e323dfd52aaf1f80c9880b35e7b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/AC_RunActiveContent.js	8	ddbe3d60fbf2c4033052fd0400201501
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/bubbleup_split.js	2	c29361dd438ce12cd65255e9482331c9
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/common.js	1	92f1e11452c15d8e5e7fd002d805039e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/dialog-min.js	19	fc8d9a82f2768f7b723717fac630089d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/dialog-plus-min.js	25	d69f20732012676b603c337eb17cf8b0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/jquery-1.8.3.js	260	2073df88a429ccbe5dca5e2c40e742b4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/matter.js	31	3a3171e0fb173023e9346ee5c3a310d2
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/menu.js	1	b0af60e3b45bfaeca4346a6ae3f0e79c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/menujs.js	1	3b8af837ec9c308576abb14b107267df
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/qyzc.js	1	8e0544278a7419a681bf5edbe81f7a10
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/regionStyle.js	2	ef314d8ceac879532d6b02a1bc8d760a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/scroll.js	1	5bcb4ea82285c79099910c1f04515de6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/swfobject.js	7	2469e471605d9332292f26ae734b610e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/swfobject_modified.js	22	6b21d8c2c636c037a41c9417e40050ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/tab.js	2	25726261f49f91d7dc9e6b884f73b91a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/tab-ㅏi ㄴ┤.js	1	2b40d26d162ac78cdae0d144d84844a9
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/newjs/wordscroll.js	3	cc51cec580e0efbcab56bcd3fedcdc33
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/qzqd/Scripts/swfobject_modified.js	22	185ca089bc9c4f94b5a1ef9ca6528acc
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space/js/bootstrap.js	57	5e4c3542c8a1d995de4bba1700fadefd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space/js/jquery.autocomplete.js	12	05c658f4fc1f839033e7b023113b0ba5
/WebHallCMSV3.0BAProject/WebRoot/r/cms/	7	91bccf1ff80aea85d5482bdf8f7a50c3

www/blue_webhall/space/js/jquery.PrintArea.js		
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space/js/jquery.ztree.all-3.5.js	117	e432136ab0b475fd5f569bdd20c8de17
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space/js/jquery.ztree.core-3.5.js	55	4c3c87522be5efcb622a927099846b0e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space/js/jquery-1.8.3.js	260	2073df88a429ccbe5dca5e2c40e742b4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/bootstrap.js	57	5e4c3542c8a1d995de4bba1700fadefd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/jquery.autocomplete.js	12	05c658f4fc1f839033e7b023113b0ba5
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/jquery.PrintArea.js	7	91bccf1ff80aea85d5482bdf8f7a50c3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/jquery.ztree.all-3.5.js	117	e432136ab0b475fd5f569bdd20c8de17
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/jquery.ztree.core-3.5.js	55	4c3c87522be5efcb622a927099846b0e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/js/jquery-1.8.3.js	260	2073df88a429ccbe5dca5e2c40e742b4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/new/js/dialog-min.js	19	fc8d9a82f2768f7b723717fac630089d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/new/js/dialog-plus-min.js	25	d69f20732012676b603c337eb17cf8b0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/new/js/index.js	1	d7d92b03310a09e0548958b3e1a601e6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/new/js/menujs.js	1	3b8af837ec9c308576abb14b107267df
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/new/js/tab.js	1	ff8110257c8b0b329bd69498e9d788c5
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ar.js	3	40da453f064e827338eac90d9c89294e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/az.js	2	af1ec6e1dd2f328c7cd29d65713c872b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/bg.js	3	3c2b485c8deaf5f3e996486b93dab8cb
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/bs.js	2	fde5829ad56ee07792e2795ae9930ca3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ca.js	2	230873c05c9672157b4dfc09f93e78f9
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/cs.js	2	429ba633ae416782a45d15440b567c98
/WebHallCMSV3.0BAProject/WebRoot/r/cms/	2	49320feb6625a149de7f2e09fa05c18

www/blue_webhall/space2/plupload/i18n/cy.js		e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/da.js	2	76d042f6c09e86af7cb0703865903d7b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/de.js	2	e762ae600cafd4841b2a1e0d2f026ec1
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/el.js	3	80ef40ba27474ae30925f00643ea8982
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/en.js	2	3240c8824ef3c835eb5badc4aa10d55b
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/es.js	2	ecb127a2290cd80143ef936f40fc707c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/et.js	2	0586d3db5ef9817bfc627d30bb228edf
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/fa.js	3	78d1ec5f9f9e1c1fcb99cf77f2982b17
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/fi.js	2	4d2c821dae08d8a947ff9626762000a7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/fr.js	2	6690e68e08ac6570a230eb330bcfc448
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/he.js	2	4b355df7402a3d2f6659c7fb92d48079
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/hr.js	2	f24024aac4743da11342383ed66d77f3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/hu.js	2	478ccff332991044c514216abe75dbd0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/hy.js	3	7226f1cd498dc6e2ebde4ac84e634829
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/id.js	2	c9ec021a60410c6316041ce1ab745986
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/it.js	2	79b1c53066d89606cd611262b80e0656
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ja.js	3	78d756164da51294ec2d45bf73663d08
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ka.js	3	c536a7476f3f6fb868a4f1ba9e8e8213
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/kk.js	3	ae7e2e1954817abef87987ce4cb1c721
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/km.js	3	cca4f0fd61771f89792fe023b0729104
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ko.js	2	c68920c34f89b01b42167cabebaad970
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ku_I	3	ca5bb4e1a2d47d631355736f2b9d882f

Q.js		
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/lt.js	2	201b3c92fc280eb31601451007c9759e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/lv.js	2	f07d386490ad776ac77a5953cff8b042
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/mn.js	2	9aea8a852ba61cfe4a9bc1f3371da3ac
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ms.js	2	4ad6f23c71163037f9ea8add0c5fee80
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/nl.js	2	36ba96f1ac9bd03ce18fa4999e96a735
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/pl.js	2	8c6645b2cabc99be9fd2feea4c8080a2
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/pt_BR.js	2	fc306a46ac070e7930ea41192cebc865
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ro.js	2	72933c4e9b4ce0251f8046e29651e745
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/ru.js	3	4e474aac4e8a00b3efcfaa1c9ec4281a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/sk.js	2	e24904d971110228794c232cdaa6bb85
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/sq.js	2	e929f1a011cad38dbfb74b1bfc714fb6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/sr.js	2	7447ab8d6593ef76eb0838b2242c453c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/sr_RS.js	2	3e15e591d1ee2ac7bf7e19ac5941afec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/sv.js	2	42de53f2ad778f3230ae58e02ee66087
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/th_TH.js	3	c9a3f8b8464a3084aa6bd46149fe0991
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/tr.js	2	94ed3e610ed179b0cde4acd438155fa3
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/uk_UA.js	3	35fc857d6a4b292acdb6454e05188e7c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/vi.js	2	e2aa18047df8bbc4a96cda78228a4563
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/zh_CN.js	2	da8ef044393f88566ca9da9f36e8a0d4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/i18n/zh_TW.js	2	785f13f951efbc045f5558b5b2ee4119
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/jquery.plupload.queue/jquery.plupload.queue.js	16	c0e8d7313cc6d1c71157aa8cffc238d9

/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/jquery.plupload.queue/jquery.plupload.queue.min.js	10	cc2299ab0a3d8b688faeffaca753faf4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/jquery.ui.plupload/jquery.ui.plupload.js	38	eb50fbf1199fc5ad86306e9735fe8b89
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/jquery.ui.plupload/jquery.ui.plupload.min.js	28	7464c8bb2473f85b42500dd15e76c00a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/moxie.js	279	988ce3f4bcdaffe236dd05a76bbcfaf4
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/moxie.min.js	148	b436a09094af40114f42ee3a2bb6ec49
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/plupload.dev.js	58	70c48c53d1e4ade2d965e5753389c24f
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/plupload.full.min.js	182	8988fe6b194c5485ae4760c69ed3b38d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_webhall/space2/plupload/plupload.min.js	29	40d4fce5dee812158078bfcfdc8047ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/common.js	1	bcbbed23ee7018ae1ef7fb91243ffe56
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/heiphoto.js	40	8058f0e0b741c7fd14992261a6b8f8ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/message.js	4	f08530cb346e45d3941fc819b14f4363
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/p-cr.js	57	d957933ea645c85687be1b3c9ecd8883
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/p-cr1.js	56	67fb4458711f487f9ffc88bd497ce6ee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/sinaflash.js	7	3a1ff60f956d80dc9f4cda3611bf754d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/js/tab.js	1	0906723e6df6db37d3b4cc64d7013814
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/index.html	1	2ccd8a4a9ee6faca2ada3c63a0782fa5
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/left.html	7	0138e7c97cb46b0c36e1ce68ab8db1b0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/main.html	2	b6c86b8f3749c5246d5b6ac1e939bfc0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-a.html	2	a5e29f5cc8e9636f02d0dbe1d3b35a48
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-b.html	1	b4cddac58dc86e5d3ae35f60867203f7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-c.html	1	166d88435e907158c1d2799b08338fc7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-d.html	1	bce62a9fd29a3cd799ce9bb26bc5cc6c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-e.html	2	49cacc2cd3db44c6c8e4110280a14fed
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-f.html	3	8a6f2644c0c85214908b5c2310e24990

/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g1.html	3	e7994ec29fae4e276277ee64baa016ce
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g10.html	3	01934ec4eb68be39150b16bb8a366986
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g11.html	3	46f781fe73b71b99f337dd52efd58795
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g2.html	3	42fd7a8cbe0e0b1c406c767a676374fd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g3.html	2	3cfaab7361da2176b4d501378d5132bb
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g4.html	2	7d1916e684089cc0ad59f7fe3326942a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g5.html	2	8a3b609bc1e50a9ecd31d9c01c65a718
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g6.html	2	d136beb653fd9ad947decfd34ebf6315
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g7.html	3	a3e787f5b6881417614ebe018f27a68f
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g8.html	3	f0ee8233ba038d6f8d073b39fb0c477c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-g9.html	3	d2418369b0b96af2534209d1cbd0c658
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h1.html	1	44d01c7aecb4a51eb28a88c5d77dcb47
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h2.html	1	88a5956c82b892ee36a30abfd6761abd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h3.html	1	3ef91e6ec2d5ef0259eab39c1462457e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h4.html	1	df1fa27d402d69cd051d38bff111d663
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h5.html	1	3fe01dbb7ca6a0ac5ee98171f39083ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/right-h6.html	2	b6d47e61d8420515d21fabdf45c55f84
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/navigation/top.html	1	cd783f270574a9aa1285ceac9deaef0e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/common.js	1	92f1e11452c15d8e5e7fd002d805039e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/menu.js	1	b0af60e3b45bfaeca4346a6ae3f0e79c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/qyzc.js	1	8e0544278a7419a681bf5edbe81f7a10
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/scroll.js	1	5bcb4ea82285c79099910c1f04515de6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/swfobject_modified.js	22	6b21d8c2c636c037a41c9417e40050ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/blue_website/newjs/tab.js	1	8e0544278a7419a681bf5edbe81f7a10
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/common.js	1	bcbbed23ee7018ae1ef7fb91243ffe56
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/heiphoto.js	40	8058f0e0b741c7fd14992261a6b8f8ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/message.js	4	f08530cb346e45d3941fc819b14f4363

/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/p-cr.js	57	d957933ea645c85687be1b3c9ecd8883
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/p-cr1.js	56	67fb4458711f487f9ffc88bd497ce6ee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/sinaflash.js	7	3a1ff60f956d80dc9f4cda3611bf754d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/red/js/tab.js	1	0906723e6df6db37d3b4cc64d7013814
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_hr/js/tab.js	1	0ee462565d3b41aca64fd324085a4902
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/common.js	1	bcbbed23ee7018ae1ef7fb91243ffe56
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/heiphoto.js	40	8058f0e0b741c7fd14992261a6b8f8ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/message.js	4	f08530cb346e45d3941fc819b14f4363
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/p-cr.js	57	d957933ea645c85687be1b3c9ecd8883
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/p-cr1.js	56	67fb4458711f487f9ffc88bd497ce6ee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/sinaflash.js	7	3a1ff60f956d80dc9f4cda3611bf754d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/js/tab.js	1	0906723e6df6db37d3b4cc64d7013814
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/common.js	1	92f1e11452c15d8e5e7fd002d805039e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/menu.js	1	b0af60e3b45bfaeca4346a6ae3f0e79c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/qyzc.js	1	8e0544278a7419a681bf5edbe81f7a10
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/scroll.js	1	5bcb4ea82285c79099910c1f04515de6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/swfobject.js	7	2469e471605d9332292f26ae734b610e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/swfobject_modified.js	22	6b21d8c2c636c037a41c9417e40050ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_research/newjs/tab.js	1	2b40d26d162ac78cdae0d144d84844a9
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/common.js	1	bcbbed23ee7018ae1ef7fb91243ffe56
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/heiphoto.js	40	8058f0e0b741c7fd14992261a6b8f8ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/message.js	4	f08530cb346e45d3941fc819b14f4363
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/p-cr.js	57	d957933ea645c85687be1b3c9ecd8883
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/p-cr1.js	56	67fb4458711f487f9ffc88bd497ce6ee
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/sinaflash.js	7	3a1ff60f956d80dc9f4cda3611bf754d
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/js/tab.js	1	0906723e6df6db37d3b4cc64d7013814
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/index.html	1	2ccd8a4a9ee6faca2ada3c63a0782fa5

/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/left.html	7	0138e7c97cb46b0c36e1ce68ab8db1b0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/main.html	2	b6c86b8f3749c5246d5b6ac1e939bfc0
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-a.html	2	a5e29f5cc8e9636f02d0dbe1d3b35a48
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-b.html	1	b4cddac58dc86e5d3ae35f60867203f7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-c.html	1	166d88435e907158c1d2799b08338fc7
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-d.html	1	bce62a9fd29a3cd799ce9bb26bc5cc6c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-e.html	2	49cacc2cd3db44c6c8e4110280a14fed
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-f.html	3	8a6f2644c0c85214908b5c2310e24990
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g1.html	3	e7994ec29fae4e276277ee64baa016ce
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g10.html	3	01934ec4eb68be39150b16bb8a366986
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g11.html	3	46f781fe73b71b99f337dd52efd58795
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g2.html	3	42fd7a8cbe0e0b1c406c767a676374fd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g3.html	2	3cfaab7361da2176b4d501378d5132bb
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g4.html	2	7d1916e684089cc0ad59f7fe3326942a
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g5.html	2	8a3b609bc1e50a9ecd31d9c01c65a718
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g6.html	2	d136beb653fd9ad947decfd34ebf6315
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g7.html	3	a3e787f5b6881417614ebe018f27a68f
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g8.html	3	f0ee8233ba038d6f8d073b39fb0c477c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-g9.html	3	d2418369b0b96af2534209d1cbd0c658
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h1.html	1	44d01c7aecb4a51eb28a88c5d77dcb47
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h2.html	1	88a5956c82b892ee36a30abfd6761abd
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h3.html	1	3ef91e6ec2d5ef0259eab39c1462457e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h4.html	1	df1fa27d402d69cd051d38bff111d663
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h5.html	1	3fe01dbb7ca6a0ac5ee98171f39083ec
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/right-h6.html	2	b6d47e61d8420515d21fabdf45c55f84
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/navigation/top.html	1	cd783f270574a9aa1285ceac9deaef0e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/	1	92f1e11452c15d8e5e7fd002d805039

www/yellow_webhall/newjs/common.js		e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/menu.js	1	b0af60e3b45bfaeca4346a6ae3f0e79c
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/qyzc.js	1	8e0544278a7419a681bf5edbe81f7a10
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/scroll.js	1	5bcb4ea82285c79099910c1f04515de6
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/swfobject.js	7	2469e471605d9332292f26ae734b610e
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/swfobject_modified.js	22	6b21d8c2c636c037a41c9417e40050ad
/WebHallCMSV3.0BAProject/WebRoot/r/cms/www/yellow_webhall/newjs/tab.js	1	2b40d26d162ac78cdae0d144d84844a9
/WebHallCMSV3.0BAProject/WebRoot/register.html	17	f80b02cccd3e56c881e451dbb70449a1
/WebHallCMSV3.0BAProject/WebRoot/res/common/js/jquery.ext.js	3	12f3a1ad7474d8ec70c1658b2840c719
/WebHallCMSV3.0BAProject/WebRoot/res/common/js/jquery.imgareaselect.js	17	5f1941a9d133e9971f347997c0a27a67
/WebHallCMSV3.0BAProject/WebRoot/res/common/js/jquery.js	320	f6b144c2ba0a9ea9f6b88ee677d58bc0
/WebHallCMSV3.0BAProject/WebRoot/res/common/js/message.js	4	9429f9a05471de3a524eb731e71f9e70
/WebHallCMSV3.0BAProject/WebRoot/res/common/js/pony.js	4	fb1e5faa14364583c210d0589e578b02
/WebHallCMSV3.0BAProject/WebRoot/res/jeecms/js/admin.js	1	1ed03c861e082f5e265e9ed5eac49917
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/common/fck_dialog_common.js	10	2ec32413af8537a74c7fd216dd421d4b
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_about.html	6	31d74db88cfcf046f19256a186450d41
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_anchor.html	6	4da7dbe7ecd76b8f8fbeeafd459e52c4
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_button.html	3	174e15d6eb529701c44b5c166daf958a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_checkbox.html	3	6509d38b5924384de0645b7811627064
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_colorselector.html	5	37267bdd878c30532b6f19330471bd02
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_div.html	11	bee5908800b92d12c373812554ebe108
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_docprops.html	22	fc7d6c996aaa64e74b92515527d44424
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_docprops/fck_document_preview.html	3	d95126c2f69af551d5ccbd79cb410b01
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_flash.html	6	b6745c824a6445fa47677a97e7880f54
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_flash/fck_flash.js	8	d6fe4c911b053f05122a4b44af081a25
/WebHallCMSV3.0BAProject/WebRoot/thirdpar	2	676eae17bfbe69619c3b403b4a0d23

ty/fckeditor/editor/dialog/fck_flash/fck_flash_preview.html		20
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_form.html	3	7f53d1ee8ea1e7343b7b8466d64e2002
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_hiddenfield.html	3	a5c7f8206eb6a5c4b655453c457e61d7
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_image.html	10	fbc2a221b1eb4aba0b01aa288fa6bfaf
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_image/fck_image.js	13	14aed4d487e0036aea497c0ff658433e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_image/fck_image_preview.html	3	4b3b69a5f4d7f05b204f5b0c764c76c9
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_link.html	13	3327ed863e6c4984d489e8c584737fb3
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_link/fck_link.js	25	08c93e790adfc92c7eb5442fc00fa8cc
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_listprop.html	4	c30852b51d3cc410e6ef2f72f39f386e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_paste.html	12	35526a8c6ee5239c7ec09a05c2f0f2ca
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_radiobutton.html	3	f30e95756707b239032b5845709013ff
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_replace.html	17	91381de0541aea8ca30086865341cca1
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_select.html	6	2e016e46c2a135ffe164765afd58099c
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_select/fck_select.js	5	a86f763794e8da7914ffd99d8b5916a3
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_smiley.html	3	8f9c3a7144e23cc9cc7f1497717c50d2
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_source.html	3	495676412d235bd8f5688b92a969c1a2
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_specialchar.html	5	bd1252c41811eac714fac6b2c606342d
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages.html	3	6cc76d686dddad6c8a421a74b8cee3cf
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/blank.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/controls.html	4	37d322670133f4f94fb66cfb266a6015
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/controlWindow.js	3	91e21ae3e7041d2c3f414faffa6d84be
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/server-scripts/spellchecker.php	6	7f22cec48b1b45262a34391eee02baeb
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/sp	5	aecc22bef2d6580e1655a2218cb21053

ellerpages/server-scripts/spellchecker.pl		
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/spellchecker.html	3	be5da5c367c9112656b38208e49fee3a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/spellChecker.js	14	5689f2777b18ec2d768f34b65f2aa74a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_spellerpages/spellerpages/wordWindow.js	7	b3bfdb51c7e491f34b21db67278bd8e6
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_table.html	14	6401cbce9fd93ced6df6115404a50593
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_tablecell.html	10	73cf8edc1d6c0d5b7fcefb25ad4f07cf
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_template.html	6	a40f0c8e32cab4a94cb4aa310b95a196
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_textarea.html	3	4ca0dce97bdd069311ad9dd05b803ef6
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dialog/fck_textfield.html	4	08af0edcc332a9ba42996cfa1785979d
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dtd/fck_dtd_test.html	1	667c96a8c41ca060bd971c06b48675b8
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dtd/fck_xhtml10strict.js	4	f49c7b1342e72415faa857e9b8eb354e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/dtd/fck_xhtml10transitional.js	5	8f78fa3131db9c72a9692be5dd63326f
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/fckdebug.html	4	ef07ac914864a22b5bea7ab9bbd62440
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/fckdialog.html	22	29ffe1701a59a6f6f879c5fa9b530873
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/fckeditor.html	12	3a068d0d2a5c750a460075c25ec0c2fa
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/fckeditor.original.html	17	20625a4362568e3586c3e0265da47c35
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/browser.html	6	e50547c8f67699f7376c8c94b7d67233
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/frmactualfolder.html	3	afb2d985f7e8c92a6a4a131dcb677321
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/frmcreatefolder.html	3	2f15deba8eb89a96c94fc4d3c7dfcf9c
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/frmfolders.html	6	6532669144958e8fab6402aa194b7d6e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/frmresourceslist.html	5	6398290069ac8ade07505aa5b5efbe1a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/frmresourcetype.html	2	f82165abc67f478cdb398ec8831fd798
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/defau	4	c039b770a1f83efb4d02aba5c8478520

lt/frmupload.html		
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/js/common.js	2	a86c42599653cc9f1812724b9c24d4dc
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/filemanager/browser/default/js/fckxml.js	4	8849edde7a2bdca6431dd390751733f8
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckadobeair.js	5	36861910333169a5e5e10f399880f637
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js	256	1742d6bf3f0b4aae3538719887bb92ed
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js	258	14af032d2ace929537dacd4e3bd5e36d
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/lang/en.js	18	6a3fb2da1592626b47c67838b083f6ee
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/lang/zh.js	17	962ed0c47e7d7b1f914174d880a50125
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/lang/zh-cn.js	17	aa83f6ca66ec06e2186f5d848915df4e
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/fck_media.html	6	f4e2166083146614c4beee7f6cb4c6cd
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/fckplugin.js	9	0793ef40cf35b10dcc0cfcde2bc5f2e4
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/js/fck_media.js	9	d3a85990295016e80ddd0fab6d5b9b32
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/js/fck_media_inc.js	6	1ad2c73be75a29fb74a34b0af41da730
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/js/fck_media_preview.html	2	4b77ec35d2ff464e3ccc31aae1f57e2d
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/lang/en.js	4	adf34dd44409f1af7b9a05e3d3bb1dac
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/Media/lang/zh-cn.js	4	127f4f924d5032b1a697b1afbfbcb3c0
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/plugins/simplecommands/fckplugin.js	2	9535205ff03eff3652677f42c0e86140
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/skins/default/fck_dialog_ie6.js	3	0a15689a2b3b89b4e2e8cc651f7483ed
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/wsc/ciframe.html	2	7e18dc59cd1ee630faca208fd19c47e1
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/wsc/tmpFrameset.html	3	49c91d622f3bad786f0c3202ab17b7a9
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/wsc/w.html	6	3e94cc34f6f0592bb4348726c46fb58c
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/fckconfig.js	14	2403d4d1a89ce5addffa88b240caa927
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/fckeditor.js	10	6ce5e05760817e8ea4c1bf273117eb5e
/WebHallCMSV3.0BAProject/WebRoot/thirdpar	4	04e073607676f0b865bdac54e9da52

ty/fckeditor/fckstyles.xml		d8
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/fcktemplates.xml	3	e336a606aa02c8be3059762bcdf786f5
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/myconfig.js	2	7f40fc0b3202e11d4ea1d7ea31f68918
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/calendar.js	18	c0d949dc804dd5972df55b6250eb34dd
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/config.js	1	d0052254a01d85f6aed5ccb7df7e5aa8
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/lang/en.js	1	e711ae181ddfc1b561e60cc55f428b68
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/lang/zh-cn.js	2	9a4c9b49b4c653461f70c7af348fd61b
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/lang/zh-tw.js	1	b8facba48fed75a3c9050653d4846d03
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/My97DatePicker.html	2	c6f42da5901bf724d55e821e438dfc67
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/My97DatePicker/WdatePicker.js	8	73d9a5b97cebc978abb04164df76ba51
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/swfupload/fileprogress.js	7	73a891cc9df8fc04a2351e1590e962f8
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/swfupload/handlers.js	7	8dcef3d5d033f17b00e9d5d60acc73dd
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/swfupload/swfupload.js	37	b21e4629bd59f26d1a0a7f2e79f5e094
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/swfupload/swfupload.queue.js	4	cb131696cf8dbfc74c675b660f4866d7
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/dialogs/attachment/attachment.html	3	c110df21e5ecc82c3806e0f25dc57d3c
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/dialogs/attachment/attachment.js	30	b5ab96476758514a98fbc154e8c23179
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/dialogs/internal.js	3	0ad353924c6424d5359aa5c8a9128897
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/jsp/controller.jsp	1	7bc0d045d2d97824d012335166c9660a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/lang/en/en.js	29	88cb6326d0cf22c4b75c847b39311767
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/lang/zh-cn/zh-cn.js	29	2a36743b9924ca0659ebaa359260e1f5
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/codemirror/codemirror.js	155	bb17a634a67754684b3df3f361db4ae1
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/jquery-1.10.2.js	267	91515770ce8c55de23b306444d8ea998
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/jquery-1.10.2.min.js	158	244340c359c83d60d2e908d09e88aae5
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.custom.js	194	ee305c10a48030b2cb303c29e1a6c8a2
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.custom.min.js	90	2fed416ed2b93626c451d250166e4c15
/WebHallCMSV3.0BAProject/WebRoot/thirdpar	136	c4a3bf9b5186325ae81a0c459f14798

ty/ueditor/third-party/webuploader/webuploader.flashonly.js		a
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.flashonly.min.js	62	99f2d2fb9a421873c2d6ebf81e3acee4
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.html5only.js	183	2cdc7bb54db94e5c8f842da451b46e93
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.html5only.min.js	87	daa589d6b8f2a4cd88ff18d890940eca
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.js	227	6c75aae8048de3d23cee4b255278a437
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.min.js	110	f4f1cad4170e5e279bf06fd9e8c559bb
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.withoutimage.js	149	ac30cd2e245e5988d8cfb2dc6f185ec2
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/webuploader/webuploader.withoutimage.min.js	73	cbb47949cd9e08449f1985e9c03e5af1
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js	43	56acbc88efd2b5c82448f8db32f1efa9
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.min.js	30	c3697e61a66416a74795f9be1414dff4
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/ueditor.all.js	1,086	3860f22164dfcc27de313ba575a5952b
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/ueditor.all.min.js	709	01191c53b5f79ae5c084f5ac528b9481
/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/ueditor.config.js	19	5db3bd2860c49644ac4bd7e12af5ca45
/WebHallCMSV3.0BAProject/WebRoot/u/sign.html	3	b09f7fc510237dbf58300b1c286ffcf2
/WebHallCMSV3.0BAProject/WebRoot/version.xml	1	14c6e3962714a042bfdb8066d73e9498
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/action/member/Service.properties	2	729f29e3c652a380e68a1f4dada77ae4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisition.hbm.xml	4	07a5e3c23419a4a2e1c87d5d306aad9a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisitionHistory.hbm.xml	1	0da9d1db0700aa1a198d588735066e67
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsAcquisitionTemp.hbm.xml	2	2978ec00c26bfa28139fa19ceaefe613
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	e3584b9e58472f5a7e89879ff2ce865

INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsAdvertising.hbm.xml		c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsAdvertisingSpace.hbm.xml	1	ec3743970cf9703c13c29274e94e3e7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsComment.hbm.xml	2	d973053ed2b25bd98059ac9a559d7244
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsFriendlink.hbm.xml	2	cba76d4ee7fba07d9e711d60ba1d94c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsFriendlinkCtg.hbm.xml	1	9bb5af460f6862fbbc863d7df4d84402
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbook.hbm.xml	2	27b1010d765e930656f8e02df8edd6ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbookCtg.hbm.xml	1	91c737657cc3c0e9b5755a4f52fc3dae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsGuestbookExt.hbm.xml	2	1997712ce98b1325ae08fd0c8c1b9a2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsKeyword.hbm.xml	1	4f17d895cfc2019616fe9b298e518408
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsMessage.hbm.xml	2	18af079d549e1025c224258256d999d2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsReceiverMessage.hbm.xml	2	12063a668e2a3002525b64b0bedea9ae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsSensitivity.hbm.xml	1	45f7f7f8cc500f1d60535bcd26a0b241
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsSiteFlow.hbm.xml	2	09b3ba5c720b6073b213298cf26d939e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteItem.hbm.xml	1	a5d8598ed2b4823c8e6d69ee2236caa0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteRecord.hbm.xml	1	f6ee83f7726df69e9d0fc3a7120533e2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_db2/CmsVoteTopic.hbm.xml	2	5b973992faae627b6e008e62177b691a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisition.hbm.xml	4	a56b8649837fa97492d36ef401053bc1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisitionHistory.hbm.xml	1	33b4da3bc005c0840dbeea7ce57a12b3

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsAcquisitionTemp.hbm.xml	2	fba2e6072bf6e453b7da705b34bf9527
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsAdvertising.hbm.xml	2	c6511bc0babedb718d56a35d00161920
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsAdvertisingSpace.hbm.xml	1	16a7c9a9aa0a4d08379e384fc0fe94b8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsComment.hbm.xml	2	01336b2d3e8d3c08ca085d6fbf91ea03
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsFriendlink.hbm.xml	2	ce1e847be74ecb632a237bf7e36d8432
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsFriendlinkCtg.hbm.xml	1	c821b5e943e8253f1f7193e46a752709
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsGuestbook.hbm.xml	2	66dcc174f96232efe27ac951fefa47ee
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsGuestbookCtg.hbm.xml	1	34336c85796f5a4a3dc694cd27cafcf8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsGuestbookExt.hbm.xml	2	1997712ce98b1325ae08fd0c8c1b9a2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsKeyword.hbm.xml	1	33c709d02b6c7e933cf0dc5d8ed3db2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsMessage.hbm.xml	2	5c26e2783a38193ee674712e2ce109a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsReceiverMessage.hbm.xml	2	27a16419cc3a1047b68270a88aaa021e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsSensitivity.hbm.xml	1	8f89158f27bb74ab9cb36594c3f2d434
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsSiteFlow.hbm.xml	2	b7f232d9138169d0763cd609ba3401fd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteItem.hbm.xml	1	e2f552f583a6b6eb4ec105070a95528a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteRecord.hbm.xml	1	b50ad1d53746b3f0d37414a60d3c8f61
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_oracle/CmsVoteTopic.hbm.xml	2	076b3fa6ebf41428c237c431da3fd7f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hb	4	07a5e3c23419a4a2e1c87d5d306aad9a

m_sqlserver/CmsAcquisition.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAcquisitionHistory.hbm.xml	1	0da9d1db0700aa1a198d588735066e67
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAcquisitionTemp.hbm.xml	2	2978ec00c26bfa28139fa19ceaefe613
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAdvertising.hbm.xml	2	e3584b9e58472f5a7e89879ff2ce865c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsAdvertisingSpace.hbm.xml	1	ec3743970cf9703c13c29274e94e3e7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsComment.hbm.xml	2	d973053ed2b25bd98059ac9a559d7244
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsCommentExt.hbm.xml	1	4a602eac7edced63f79bf711466f6a70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsFriendlink.hbm.xml	2	cba76d4ee7fba07d9e711d60ba1d94c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsFriendlinkCtg.hbm.xml	1	9bb5af460f6862fbbc863d7df4d84402
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbook.hbm.xml	2	27b1010d765e930656f8e02df8edd6ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbookCtg.hbm.xml	1	91c737657cc3c0e9b5755a4f52fc3dae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsGuestbookExt.hbm.xml	2	1997712ce98b1325ae08fd0c8c1b9a2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsKeyword.hbm.xml	1	4f17d895cfc2019616fe9b298e518408
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsMessage.hbm.xml	2	18af079d549e1025c224258256d999d2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsReceiverMessage.hbm.xml	2	12063a668e2a3002525b64b0bedea9ae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsSensitivity.hbm.xml	1	45f7f7f8cc500f1d60535bcd26a0b241
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsSiteFlow.hbm.xml	2	09b3ba5c720b6073b213298cf26d939e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteItem.hbm.xml	1	a5d8598ed2b4823c8e6d69ee2236caa0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteRecord.hbm.xml	1	f6ee83f7726df69e9d0fc3a7120533e2
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	5b973992faae627b6e008e62177b69

INF/classes/com/jeecms/cms/entity/assist/hbm_sqlserver/CmsVoteTopic.hbm.xml		1a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CConfigBase.hbm.xml	1	929faa5c9ef04303eda2e7f275c69235
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CCooperateBusiness.hbm.xml	3	e681146fa5777d16d843bc8f30d2b3ea
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/Channel.hbm.xml	3	ea4fe624593381f3c116ea86a1f5346a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsConfig.hbm.xml	4	f9a649ca7c61a6facb0c6fcbb2cde78f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsGroup.hbm.xml	2	e179c70d8a4479bf0bfd11e6d166bf25
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsLog.hbm.xml	2	2a0f90e70ef09b960fb2d81e7a270ca2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsModel.hbm.xml	2	ee231e0577df57deaf4798759a1f6bd9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsModelItem.hbm.xml	2	7032c86c11f151abf30c5b941b2f1ce9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsRole.hbm.xml	1	4c2e29d04a1ded2dfe24258d9fc14ddc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsSite.hbm.xml	4	400e5a8ba60ee446ce6061a9b2e87551
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsSiteModel.hbm.xml	2	5ef6ddac5c964aa0ca75578d87552c29
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsTopic.hbm.xml	2	86708219f6f6dca55a740f98058f2953
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsUserExt.hbm.xml	2	31471fe2cf210c9b85048f8367826449
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CmsUserSite.hbm.xml	1	97eec5a8dba6360115e5aaf246ce3159
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/Content.hbm.xml	5	18602e68f5a6d43a3e6a64707b68944b

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentExt.hbm.xml	3	8fbf3703a4884ecf1e13348a6985a636
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentTag.hbm.xml	1	7834e5a998303b0c3f727bc4cf4a6d9b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/ContentType.hbm.xml	1	4376595eacc3207c544b24c5518714f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/CoopBusinessTotal.hbm.xml	1	2b1c838bf4024be5fefd6c454312a788
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/SpaceAttachBase.hbm.xml	2	1ae022795b8cad8162f14be0f05a5d8c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/SpaceCertInfo.hbm.xml	3	b7190fa914e299df214c37d6d55608c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/SpaceClxxInfo.hbm.xml	3	d4a9253dbd203d8cdd15645d5003c9d8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/SpaceDataExtend.hbm.xml	2	96b446aa2e6abb86605e21e8ea735cc0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsAdvice.hbm.xml	2	81a184010382c24ca6271f667ba14cd2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hb	1	f9eb242d965581d2d3b7e04f46afcaa9

m_db2/TInsBusinessTotal.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsWebhallBusinessInfo.hbm.xml	4	97b7dbc188b721a6cec75e05d388a62e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TInsYwpz.hbm.xml	2	e6cb612824700fbc78873ca7f1b0c8d2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TOpinionRecord.hbm.xml	1	129453867efa701f7c0641bebd612bf6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TOpinionTopic.hbm.xml	1	da7338bdc1b1cf283dc7c09b9cf55082
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TShareCertificateinstance.hbm.xml	3	1b9eecea2426ea815ce784fd2b56af59
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TShareFile.hbm.xml	3	110f4c480c7dd3de4e8aa64e05c15a7b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TShareInvest.hbm.xml	2	3824f18bf0f16303fe2bd08bd8ee2d3c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSharePermissionitem.hbm.xml	15	3e1d61363152e7392c77825de1494ac0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TShareWebCondition.hbm.xml	4	38a3953f00faac1c212d267a219114ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSpsxPermissionmapsort.hbm.xml	2	9ec62c5e7e823577a150f701cd9e7446
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	3c4e3171bb02d2b514dc666dd3ecf4c

INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSysDeptWindow.hbm.xml		f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSysRegion.hbm.xml	2	38c5624390bba6a12dbec5c4cd6655c8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebHallIncInforMation.hbm.xml	3	b4a99022c3ef3f8755bbda6794ced19c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebhallReferComplain.hbm.xml	3	23cc7fad44d1e409ca611a430951ca56
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TWebHallUserInforMation.hbm.xml	2	b9ef8114fe33b802ef23b76de323f24a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/TXmlClob.hbm.xml	1	9dce5aae665669d2fd1a249715de1fb6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VCooperateBusinessinfo.hbm.xml	2	cd025c7add95ad2c15fb66a19bd23729
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VShowPermissionitem.hbm.xml	3	1bf43a7b039ea14d8dd958775997c06a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VSortPermissionitem.hbm.xml	3	4a5ee4532323ecc6fe89c9e0e4899586
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTInsAdvice.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTInsBusinessinfo.hbm.xml	2	f2032c1dd0bedd21996511cce64d5993

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTInsWebhallBusiness.hbm.xml	2	6e68932acb17dfa7ba26cc72ff032d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTSharePermissionitem.hbm.xml	1	d919f25276bfb4ce08a8c9a364c06881
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_db2/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CConfigBase.hbm.xml	1	0a4a6f2001cb6cfe28969daf5e8de6a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CCooperateBusiness.hbm.xml	3	89d84427f3ff60de2b1580d723f0ce98
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/Channel.hbm.xml	3	6de5e4fdf96deaab9775275a6f7e90c2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsConfig.hbm.xml	4	d02dc141778e080e7aff27a2ab81d38b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsGroup.hbm.xml	2	0387220e2d89c3af5b9a5c973319d4c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsLog.hbm.xml	2	cdda119e1dc5fed30c7651862c01c25e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsModel.hbm.xml	2	0fc7f191a04a8b140108c7dd58e1fcf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsModelItem.hbm.xml	2	4137a13e8b6be0a1fe17c8f30799094b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsRole.hbm.xml	2	76320a9a80a1cef2bdbea815252af760
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsSite.hbm.xml	4	d33c333fee35a3a15cb16d97692fd72c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hb	2	22cd375f7e7315d1e987c0baec1d440a

m_oracle/CmsSiteModel.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsTopic.hbm.xml	2	a738f01cde50a9351e0702544868a2fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsUserExt.hbm.xml	2	31471fe2cf210c9b85048f8367826449
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CmsUserSite.hbm.xml	1	737056e2b2956c265636afc9f5f5e060
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/Content.hbm.xml	5	9625468c22cf5dc29eb553d9a9fa2f61
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentExt.hbm.xml	3	8fbf3703a4884ecf1e13348a6985a636
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentTag.hbm.xml	1	4bcb608317ca65f9e8c1fea48e49d9ec
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/ContentType.hbm.xml	1	32c49d639a686204912e94d0e2ef1170
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/CoopBusinessTotal.hbm.xml	1	4d2683310d9d9fc22b26f8b18692e3f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceAttachBase.hbm.xml	2	70c32e40bfa6321f0d6d37520a4d6f83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceCertInfo.hbm.xml	3	66cea0d23572bdf0824e8cd68360efee
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceCertInfoExt.hbm.xml	2	ce97858edc9763dcf5a7f70b53d11d6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceClxxInfo.hbm.xml	3	4f990996bed68f1b8bed0bb9a5e0821f
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	c7e1646f603916e0710b364ecb22b9

INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceDataExtend.hbm.xml		76
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa002.hbm.xml	3	936327bfde3c1ea5ed22a77606388813
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa003.hbm.xml	3	858e33bd3597ca95521a98b5d41e97aa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/T29e000027aa004.hbm.xml	2	fa6d7a8da6a6055a5ba5bf34e777a133
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/T29e000028aa019.hbm.xml	3	0142d8c5ac236cb5cdb872f2e172b378
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/T29e000063aa003.hbm.xml	4	27ce6a8da5ab99dd292a4a2f497185d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TFormLib.hbm.xml	3	4c033af8733dce812bf38b03deb8e323
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsAdvice.hbm.xml	2	e3dd95512190fda7897fc4d3889e64c5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsBusinessTotal.hbm.xml	1	d9078e4826fcba68e5273f598780d96f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialCompare.hbm.xml	2	030eb0a851457d3bc305c439851ecfd7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsMaterialValid.hbm.xml	3	857827b16891b336f663085d07dbbe22
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsWebhallBusinessInfo.hbm.xml	4	e2b0c1fd0302b4d45ba7a52ab248390a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TInsYwpz.hbm.xml	2	71dc96cecfb5febaf7c855952d83e096

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TOpinionRecord.hbm.xml	1	e2b8a4dd299de9b92db1305e35f39559
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TOpinionTopic.hbm.xml	2	0f52f159dad1d710cc24e41322276fd0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareCertificateinstance.hbm.xml	3	ad09edbbbbbdf23dab883cef080ece1b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareFile.hbm.xml	3	cc06dc13ae02bb25cef6fec9c7decb62
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareInvest.hbm.xml	2	3824f18bf0f16303fe2bd08bd8ee2d3c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareJdsqxx.hbm.xml	2	80cd71e6de5433facf3a15a5f5d8880a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSharePermissionitem.hbm.xml	16	be66152191dc5fcab41191e3fa941138
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareSxclgl.hbm.xml	3	e0990991d71bb3ed13988f9671bf9e1c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TShareWebCondition.hbm.xml	5	90873f1ca3c1a0cef2dbb4af61e859dc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSpsxPermissionmapsort.hbm.xml	2	a85a34840760da1e5fc80fc95ca47ab7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSysDeptWindow.hbm.xml	2	ec7cfe18075ae6960af74c4ee6621311
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hb	2	38c5624390bba6a12dbec5c4cd6655c8

m_oracle/TSysRegion.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebHallIncInforMation.hbm.xml	3	67c29bbdaf568cca9244228d2623b216
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebhallReferComplain.hbm.xml	3	97b8c7e8d3397afa8fbdbbe026d4342c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TWebHallUserInforMation.hbm.xml	2	f77c7005edbde91ff3b0fda80dda5e56
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TXmlClob.hbm.xml	2	7ff0ca5eff979e507965e3888b34b275
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/TYWLSHLog.hbm.xml	2	989640db89b06daff918e0b9b91d2a38
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VCooperateBusinessinfo.hbm.xml	2	69d500b40eddb6a005261b669ddf1c5a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VShowPermissionitem.hbm.xml	3	92e06dec08919fa693a3ff7aa9237e5c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VSortPermissionitem.hbm.xml	3	34ba0c4aafdd5b98c5f5dd223e63024d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTInsAdviceTJ.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTInsBusinessinfo.hbm.xml	2	a7731bde4a30a11a9b9a7f2ad6fe2598
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTInsWebhallBusiness.hbm.xml	2	6e68932acb17dfa7ba26cc72ff032d5e

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTMaxsxbhPermissionitem.hbm.xml	1	c7600d78cdcfdb04eed46d2e58f481ca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTMaxsxbhSortPermissionitem.hbm.xml	1	916992c20ee951b1a4e6c44c80da5620
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTSharePermissionitem.hbm.xml	2	7daff06d1980f82253fb60f7057c8ad9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageChannel.hbm.xml	2	e624b1ac4037a6d6f377a5795bd239ae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageChannelgr.hbm.xml	2	72ba436cb1dd2c7f113eda5167f0c733
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageEnterprise.hbm.xml	14	42be8f9a3548a8c2d252be8955b1970e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageFavorite.hbm.xml	2	471a89abe4055df27cee3a677a770b29
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageFavoritegr.hbm.xml	2	3874bae82a54dde5a48348685002affa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageReminder.hbm.xml	2	957630344d58f700c5d240fd992137785
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageRemindergr.hbm.xml	2	28c4491d6c2fbe3b6a55ba99d59b4d4d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageUserChannel.hbm.xml	1	e00da79034193da17867466c2f8f618e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_oracle/WebpageUserChannelgr.hbm.xml	1	b93278cfce880bf625610bff081f553b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CConfigBase.hbm.xml	1	0a4a6f2001cb6cfe28969daf5e8de6a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CCooperateBusiness.hbm.xml	3	89d84427f3ff60de2b1580d723f0ce98

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/Channel.hbm.xml	3	ea4fe624593381f3c116ea86a1f5346a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ChannelExt.hbm.xml	4	bdb4a33156fa773a45f78a823eff012b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ChannelTxt.hbm.xml	2	74fc88bd20da236d70c22f769fd9313d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsConfig.hbm.xml	4	f9a649ca7c61a6facb0c6fcbb2cde78f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsGroup.hbm.xml	2	e179c70d8a4479bf0bfd11e6d166bf25
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsLog.hbm.xml	2	2a0f90e70ef09b960fb2d81e7a270ca2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsModel.hbm.xml	2	ee231e0577df57deaf4798759a1f6bd9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsModelItem.hbm.xml	2	7032c86c11f151abf30c5b941b2f1ce9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsRole.hbm.xml	1	4c2e29d04a1ded2dfe24258d9fc14ddc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsSite.hbm.xml	4	400e5a8ba60ee446ce6061a9b2e87551
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsSiteModel.hbm.xml	2	5ef6ddac5c964aa0ca75578d87552c29
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsTopic.hbm.xml	2	86708219f6f6dca55a740f98058f2953
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUser.hbm.xml	4	ce11ab48b21a5f372035a68f0e66fab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUserExt.hbm.xml	2	31471fe2cf210c9b85048f8367826449
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CmsUserSite.hbm.xml	1	97eec5a8dba6360115e5aaf246ce3159
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/Content.hbm.xml	5	18602e68f5a6d43a3e6a64707b68944b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ContentCheck.hbm.xml	1	bd65d507846d69d3f3cc45ce8004aa64
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ContentCount.hbm.xml	3	f9782d4f4005b042b2f80b50ec1e8c90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hb	3	8fbf3703a4884ecf1e13348a6985a636

m_sqlserver/ContentExt.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ContentTag.hbm.xml	1	7834e5a998303b0c3f727bc4cf4a6d9b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ContentTxt.hbm.xml	2	4e1d4e2763b330a2b36a82c7e0315d37
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/ContentType.hbm.xml	1	4376595eacc3207c544b24c5518714f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/CoopBusinessTotal.hbm.xml	1	4d2683310d9d9fc22b26f8b18692e3f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/GongShangweifa.hbm.xml	2	13323a78c1a2f35e8d406fc4de8f66dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/QRTZ_TRIGGERS.hbm.xml	2	533f149a571fd989af398ab8d469e1e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceAttachBase.hbm.xml	2	dee69b99afbfd65ad83dd8bc3f25361f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceCertInfo.hbm.xml	3	b7190fa914e299df214c37d6d55608c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceClxxInfo.hbm.xml	3	d4a9253dbd203d8cdd15645d5003c9d8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceDataExtend.hbm.xml	2	df036f11865f9d02765a53dc91e02272
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/SpaceDataExtendValue.hbm.xml	2	f983a32929c57c1f3839504d8088df4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TFlowNode.hbm.xml	3	e5e878a64e037f6adb2d5b766707e411
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/THrUser.hbm.xml	3	b3bd9d603255b75436fc86f1538985fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsAdvice.hbm.xml	2	81a184010382c24ca6271f667ba14cd2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsBusinessExt.hbm.xml	2	82f6e7c3c26ed59b9b47dabd9114700b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsBusinessTotal.hbm.xml	1	d9078e4826fcba68e5273f598780d96f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsFormData.hbm.xml	2	4dd7b242124f7e99e9791063fd8105c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsMaterialInfo.hbm.xml	2	e1c00fc0d8741fb09f9f12e83031db3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	97b7dbc188b721a6cec75e05d388a6

INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsWebhallBusinessInfo.hbm.xml		2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TInsYwpz.hbm.xml	2	e6cb612824700fbc78873ca7f1b0c8d2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TOpinionRecord.hbm.xml	1	129453867efa701f7c0641bebd612bf6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TOpinionTopic.hbm.xml	1	da7338bdc1b1cf283dc7c09b9cf55082
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TShareCertificateinstance.hbm.xml	3	1b9eecea2426ea815ce784fd2b56af59
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TShareClxx.hbm.xml	2	598bdb849b0ce0cbd2859f5ff5a3e8db
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TShareFile.hbm.xml	3	110f4c480c7dd3de4e8aa64e05c15a7b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TShareInvest.hbm.xml	2	3824f18bf0f16303fe2bd08bd8ee2d3c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermissionitem.hbm.xml	15	cf36ebcbdd4c6455a2300ab1ca8fd224
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermtowindow.hbm.xml	2	11b5aa94ef9390e4e30adaa45dd4f3e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePermWs.hbm.xml	2	a88e96f27d76687c7d7dbbb93f3dd07f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSharePost.hbm.xml	2	5334ffbb16a371564c887df579f7bb7a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TShareWebCondition.hbm.xml	4	38a3953f00faac1c212d267a219114ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSpsxPermissionmapsort.hbm.xml	2	9ec62c5e7e823577a150f701cd9e7446
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSpsxPermissionsort.hbm.xml	2	459ffd224b5e42fd184fce95d5556ca9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSysDept.hbm.xml	3	4f84bd900cbf808e8900d7109b3d9b5a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSysDeptWindow.hbm.xml	2	3c4e3171bb02d2b514dc666dd3ecf4cf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSysFlowlibmapform.hbm.xml	1	581270484ce7dfe02ddb12b4ef8dfed0

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSysRegion.hbm.xml	2	38c5624390bba6a12dbec5c4cd6655c8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TSysSync.hbm.xml	1	20e218c96bd795ded97a8e356422f74d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TTyspBusinessInfo.hbm.xml	2	c5a8a373f1c0d8c54704e03e8eb35784
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TTyspGrsbclxx.hbm.xml	2	522719fb92d8ac3f016388f3533ad4c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallBusinessInfo.hbm.xml	2	b3a52241bceb9e29e05d2b64e71b7e00
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebHallIncInforMation.hbm.xml	3	e670baaaf0af3acccdd927c90cf89757
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPermissionitem.hbm.xml	1	4eb397ccf53119e7e647017223cfc288
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPermissionitemPost.hbm.xml	2	25b6c394db195f9109dda1db8e1e3ad5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallPost.hbm.xml	2	b36ba2a844363e1a8e684511c18b9466
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebhallReferComplain.hbm.xml	3	23cc7fad44d1e409ca611a430951ca56
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TWebHallUserInforMation.hbm.xml	2	b9ef8114fe33b802ef23b76de323f24a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/TXmlClob.hbm.xml	2	879f436d3ced838eda9b6074464707c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VCooperateBusinessinfo.hbm.xml	2	69d500b40eddb6a005261b669ddf1c5a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VShowPermissionitem.hbm.xml	3	1bf43a7b039ea14d8dd958775997c06a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VSortPermissionitem.hbm.xml	3	4a5ee4532323ecc6fe89c9e0e4899586
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsAdvice.hbm.xml	1	a6b11543b92616352be4cb92ff2d6646
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsBusinessinfo.hbm.xml	2	3127d38279c8234fdd40f64601fb701e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hb	2	6e68932acb17dfa7ba26cc72ff032d5e

m_sqlserver/VTInsWebhallBusiness.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTInsWebhallBusinessTJ.hbm.xml	1	77ddd57d1fb0db5a66c8190e9a59e148
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTOpinionRecord.hbm.xml	2	3f00645195e6c69ded2fd0ea5eb41465
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTOpinionTopic.hbm.xml	1	5d2e51f717cb8b1565411dae7671c50a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTSharePermissionitem.hbm.xml	1	d919f25276bfb4ce08a8c9a364c06881
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/cms/entity/main/hbm_sqlserver/VTSharePermissionitemType.hbm.xml	2	009668d629067303dbd480ec0117427f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/common/fck/default.properties	1	5b3fc29e63f05a5a8dff744cc4825a87
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/common/sm/smsendsql.xml	4	b27cfba8b2a947f6a02aec64040a759a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/Ftp.hbm.xml	2	eb45eefc033c2f8a1e179084cfac96b0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_db2/UnifiedUser.hbm.xml	2	2825d95047e765324fc57ace529de209
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_oracle/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_oracle/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_oracle/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_oracle/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_ora	2	ea2a9737ba407230eeda61969956bd6e

cle/Ftp.hbm.xml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_oracle/UnifiedUser.hbm.xml	3	3eaee0a998b87db5885218abbe072785
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/Authentication.hbm.xml	1	231ef0c51eb92c5414aa7b38ad8e0e21
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/Config.hbm.xml	1	6373ce2c32c44f1bcbefe075f28e1be1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/DbFile.hbm.xml	1	e1925b41b720497f4773c22dfcf78dae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/DbTpl.hbm.xml	1	787f54caedc74bd6d129026d3d29dc43
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/Ftp.hbm.xml	2	eb45eefc033c2f8a1e179084cfac96b0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/jeecms/core/entity/hbm_sqlserver/UnifiedUser.hbm.xml	2	2825d95047e765324fc57ace529de209
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysDept.hbm.xml	3	a405199cb59dd9df6483d1dcc7420b26
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysMenu.hbm.xml	3	cbffcac05fe81bff23c4da23e0a88c8f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysRegion.hbm.xml	3	57b9199f30869089d82672bb166af4b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysRole.hbm.xml	3	9089730308b816d47294b63b57d250c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysRolepowermenu.hbm.xml	1	76d478c2999e98e9a8c2a7963cd4b2cf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysUser.hbm.xml	5	6a3401f91dcc8b42d8618029b62c1bb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/com/tjsoft/system/model/TSysUserroleass.hbm.xml	1	4b2dad5ec9c738f04676d1cfb5a6a0b1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/ehcache-application.xml	1	619d7af435973fd88bea58bfa29294a1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/ehcache-hibernate.xml	10	20f797e7dfe0a5418e455690466e28a2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/fckeditor.properties	1	56fbc690b28bbc53f4433c3aee205ab6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/logback.xml	1	e1fac0da7e0251f1a8be9168b5723f74
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/quartz.properties	2	5ea29b24af40ee970e6d8319236eecc1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/Service.properties	2	571b019743ac49f8ba56d2d6b07fa221
/WebHallCMSV3.0BAProject/WebRoot/WEB-	1	cf9683f27c598c38112bd3ae71f07aef

INF/classes/sms.properties		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/classes/smsendsql.xml	2	320c489b079a60f58a4032e35ba5c84c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/alert_message.html	1	dc605e5ec37d3d1e5f1cfe264c3ff0d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/error_message.html	1	861c76bf4d77b125ebbbd867db8b058a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/iframe_upload.html	1	096d160e83e6575f9de626cfe5949a58
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/image_area_select.html	6	b7f25af89e4de3ba51f9501ab22bc771
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/image_cuted.html	1	280dbd7fce10069e6c8328da95dc9fa2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/common/image_upload.html	3	7a4de3eba5518ea92f8c776e8fd8b067
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/application-context.xml	7	355841c097409bc7871d0dd958c226dc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/app-transaction-service.xml	1	fbd5b86c6cb7428868646daf2e1a9a5c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/cache-context.xml	2	bb4fbbd8ef5fddedfa5bad0912de4b09
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/captcha-context.xml	5	23496faab030ab542663d725df9522fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jdbc.properties	2	b6706aa1a13cff53a90dc277bcb030a6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecms-context.xml	39	4ef16d9fc2a6efd7063822154ed640bd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecms-servlet-admin.xml	5	16bd63b47cf0038ac1f8ac62c7f32ea1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecms-servlet-admin-action.xml	5	be493d7c828281e7581cbdef9ab4320c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecms-servlet-front.xml	10	79d48440958ce54e580f5ba42a0bc3b3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecms-servlet-front-action.xml	8	0b1df6f49eaac24cb1c37659ce845489
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/jeecore-context.xml	4	7baafe6e9c120da8256ad424d081a5a4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/mongo-config.xml	2	dffed6d06cea80878a6103ebf775a1c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/quartz-config.xml	1	c047e719c5b4b06143c60c13320f1954
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/rest-service-context.xml	2	bed9f41283a31be74e7a6386d96d786b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/system.properties	2	7e6a7bbb9bd44a61b8a83fd4ccba007d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/webappName.properties	1	1c7bb6b19f99dc8a99eb83a1e0bea1c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/webservice.properties	1	e4d330bce576462de999fee16095e4c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/config/webservices-context.xml	9	14daa55b581edb89551b6fb5f742dfca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/403.html	1	c25665d2b982194f12004754c5830d56
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/403.jsp	1	37745feb614476579c373f75bef42d95

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/bindException.html	1	f5584a0378efc3127f2557d66d6bb3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/integrityViolation.html	1	47e660f6821d01650da86fa90f6d7e3f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/mismatchParameter.html	1	5bc1e41ae3ad448e387e5f7b9a7a8464
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/requiredParameter.html	1	a55abf1bfe94a047f7e191f0e0979e8a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp	2	3417264d6ddfba89e16965e1c5d41dfb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/flex/messaging-config.xml	1	7183f1712ff7673ceda72028b7e2a768
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/flex/proxy-config.xml	1	6dd67e1ec66dab42ceb8c997bf5e6f35
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/flex/services-config.xml	3	42a8a0673e1478921b88ef9e0df9d130
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/flex-servlet.xml	1	945baba7d6a241e9f408ee6a3de214fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/add.html	6	3a334c060416f2cf0a1450dca01f10ee
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/edit.html	7	a1cc4512e6461466de17d4ddd7b64a11
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/history.html	4	c26c7a455e70e6dfb8a676e0b20455ce
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/list.html	4	1ed3078814f00736f51b54c23af50554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/progress.html	2	71e8f87dd5a8bf5952896f4484ce3951
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/acquisition/progress_data.html	3	88a0f0d3966a67c5f66dcf51c93ebfe8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/channels_add.html	1	257e0e109a5ad3831192808a45d5ae30
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/channels_edit.html	1	ea41b267d589a0503f2d0e8ca4ee53c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/global/add.html	7	d806ffd6b01e8a6d4edcf35b1ffbef7a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/global/edit.html	8	66a9d59fce220a318270d3d464147c4e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/global/list.html	4	54c1f32fb9d8f6b03417c5936184b54d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/local/add.html	6	1ecd81b3263e7fb6c93facc7d49b4241
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/local/edit.html	6	41a919d0387c5d298668b50a39c89d71
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/admin/local/list.html	3	02168c62c6445c71657ceac14d4c9e88
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising/add.html	7	7f0675c7ddf9defe73bcdd94d2298cf8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising/edit.html	8	430940c29a2546106b517ab3fe30af30
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising/flash_iframe.html	1	e79b8a445fc08916df4135c1991363e0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising/flash_upload.html	1	a64c4ffc8a70168c70ee97477702b5e0

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising/list.html	3	74e7a33ba407da92383f863f0df96868
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising_space/add.html	2	404aeef4236fc37fecf582a606cd535e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising_space/edit.html	2	18d051e312c4587d58b56568ead27ffd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/advertising_space/list.html	3	e9a1bd4c563745f8ffeecd0b350f90d1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/channel/add.html	14	8df9dacc031734900839090e226f67ff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/channel/edit.html	15	b3ffb450f54c1b05880aa86e04ae8a83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/channel/left.html	2	4ff9c3198276ca7ac1ff1af42ac16d92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/channel/list.html	4	f369176ee3e0babd95596c27f6c4457e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/channel/tree.html	2	7db42ab71bf797a0bbb4b3ecdf0fa4e1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/comment/add.html	1	e40ce1c879c0e25c20575b4b4f689801
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/comment/edit.html	2	1f5d921d498fe286633d715aade47bc1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/comment/list.html	3	bce16f8d3e2124fbed9181c9da8c2f88
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/config/inc_opt.html	1	32acd30eddf8225bab43a676abc8384d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/config/login_edit.html	4	958b6df0a1f07d4a86ea50fbbac9cae1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/config/mark_edit.html	4	5985212c52c50db9320ca366fcabdc82
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/config/member_edit.html	3	5ad1d9d4b966e050352ac87f02a8380c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/config/system_edit.html	2	cdb73580eea480d7c67207107f886310
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/add.html	23	6c17696f558c094abe73874b600fa230
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/attachment_iframe.html	1	fecda9ed93a876cbeebe80ca84bf75e1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/attachment_upload.html	1	68070d5cb7441e1fc5e0e6a8b4ac3c6c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/cycle_list.html	7	a7b2698f1c73183fb0d089a0b2b21a4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/edit.html	24	d2613010ef3a310962d80a11b750e44a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/left.html	2	90155698412331402bf9a360df79d7b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/list.html	12	cd663182c1ee5c25b99866dfd359249b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/media_iframe.html	1	d35221f6fa5fca95c56af304fed9ba8d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/media_upload.html	1	73105ed9d81994095e8bcd7d5d848d67
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	3a483074a34ded6c5b453cc361fd806

INF/jeecms_sys/content/tree.html		9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/tree_channels.html	2	e30a86ef6e0227f816fe0526f6ce2bcd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/content/view.html	4	ebd526f443c1d7771c2584015d8a8782
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/date.html	1	f660c828c2be62b7c328fe4701c40c4d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/assistant_left.html	3	03d63ca7fd84c5bfa80800bc35f582d3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/assistant_main.html	1	7572b5ef822793309abac2f8d5034acf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/assistant_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/channel_main.html	1	d95ca0cdf6227256d198b412afa8901f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/config_left.html	2	39b6a73e5fb13bae7323d81c2da90f30
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/config_main.html	1	d991fc07cb4ce883af2b8264deec88d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/config_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/content_main.html	1	8e5b50f175718720647c2b839235a9b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/generate_left.html	2	907713310da3030c5ab1d182362bac26
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/generate_main.html	1	608b3d5c95880c3503ecebc6e8d6d3b3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/generate_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/maintain_left.html	2	06afa7ccfe5a9e799174e65ee353d328
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/maintain_main.html	1	a27ab384a8d503536f55ba6c297cf223
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/maintain_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/resource_main.html	1	32c338b226c10b924bbdbe77b84b86b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/statistic_left.html	4	6c4de0b213200bc6fb815db42d679504
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/statistic_main.html	1	1da109f5e51412cae73897e7c3988117
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/statistic_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/template_main.html	1	dae7b5ee16623631e0964af63a5e0a01
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/user_left.html	3	d2c7a1c526281b63db567581003a0171
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/user_main.html	1	fa930a026b9fcbc2fcb9b4c363e2b516
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/frame/user_right.html	1	7f51ff009596cff3abc2410431d81678
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/friendlink/add.html	3	3f475e148772150f338903c2cee14fa9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/friendlink/edit.html	4	0d431f181ae317ccfd00a3ac68e63e84

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/friendlink/list.html	4	7a2e94c0588cd553be7fdc7cf786bbaf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/friendlink_ctg/list.html	3	6917b6fc4573edeb17a0b33c1b63276f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/ftp/add.html	3	af91aab31f1cbc39477f109802b0a825
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/ftp/edit.html	3	60817a6496301e4387405587c623d885
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/ftp/list.html	3	8df2216e344cbb50e3b8774777539a16
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/group/add.html	3	f223f09ca304e41442fb1ec9d847f3ab
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/group/edit.html	3	557b0536020a5b9a7ccf28cf157ae218
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/group/list.html	4	43fcab62888f119aec2e099cc129bf1d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook/add.html	2	58410dbb8c465feee4dd9fdfdb2a7e44
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook/edit.html	3	65e4c46dbf86bbf46c8bb4bcbb465fdc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook/list.html	3	feac5a1ed65b4824bacb2bf8766cba89
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook_ctg/add.html	2	590d25a4f592287c894761e0e6adcd22
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook_ctg/edit.html	2	d5c7ef4d7b7ed4bac6fa955795b2c51e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/guestbook_ctg/list.html	3	e655b2caefee604b1bd9a7148e954da5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/head.html	1	fe0ac54a688f39b3100c399e6704a9a4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/add.html	5	35c22f0e49e914beb24b8d285bb0394f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/edit.html	6	e97f8df46725b753da8485b67877775e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/exportByEdu.html	1	7af837d65d220241cac94772f66f916c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/exportByRole.html	1	8c9709dd919695057e711891f9c9df96
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/exportBySex.html	1	2bbfb12771ae34df8c37fedc6f53b10d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/exportByType.html	1	b52792bbabc1cc8bd81056f560ebda83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/hr_user/list.html	5	7cbaf44a3dac3b3f560fee80879013d0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/index.html	1	cd05bb072cda8ee663ab6d821ec1c296
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/item/add.html	3	4daac933241e8544cc08b0a498119848
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/item/edit.html	4	78dbfe224479d47c0caff730b9e13144
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/item/list_channel.html	32	7a2595a918484ad6aa7469580a371a32
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/item/list_content.html	29	7d2de364c20b41275bc1b1eb98f36c1d
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	50297c9fb2005cbbe517555bddfb1b5

INF/jeecms_sys/keyword/list.html		e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/left.html	1	da1db8716b31f02231142ff80cd76bc8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/log/list_login_failure.html	4	154a3b18d82e38a9fc0e63abba255774
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/log/list_login_success.html	4	2dc00abeb9691a38e1fcce15ac021a35
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/log/list_operating.html	4	a647bc228efb4e6f929c87d47f0acdbd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/login.html	6	fb80ed60f405981109a19f90e7bdd45a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/login_status.html	1	fc9b213f7e78964e66d93723b6a08738
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/lucene/index.html	3	b52e81f0455de8666337a542aaaf23f9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/main.html	1	d7dc55c88976b894702a1a020fe1aa8d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/member/add.html	4	f22d54c4bb16cce7f120cace2d3a4970
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/member/edit.html	4	eb04f223a3936c63fcc26dad99f165a5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/member/list.html	3	5b90c86c95fe9fb93e0b8f0bd1b5f127
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/add.html	3	8b6cef5e2a33edb65d7dbc8c85724f76
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/draftbox.html	3	a6d9b36b67fadca7a47e506a96facec1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/inbox.html	3	110cf778f781540d0e2a2400ada6b7f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/inc_opt.html	1	68ebea2bec2c19cb2c347346eb4bde5f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/read.html	3	9870499d60f7202198057763a9254d45
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/reply.html	2	680bc935c82d5a7fc84191ff8aaaa739
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/sendbox.html	3	850500f786dd1f1690124fc9d8c560cf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/message/trashbox.html	3	43d36744b2776f5857544a48803f6d90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/model/add.html	3	8092ddf9de9830dcbf16cfbba85d38e5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/model/edit.html	3	3563fac079e55294bca84dea21cd215c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/model/list.html	4	78e288d7fa03a82d527ba7fcaa577395
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/opinion_topic/add.html	2	3a5e351f3c1b47ef517a7de44f4a3564
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/opinion_topic/edit.html	4	8300cd41d63f63ac2d81f29dc1515175
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/opinion_topic/list.html	3	87c95301520fbaf195f67998b300bb62
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/personal/profile.html	2	77b304ecf110880d68c76c95914f680d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/refercomplain/edit.html	3	0094558417ae18104c5b19173e617e26

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/refercomplain/list.html	3	67e9175e7785eca26c29dd09a9c1216d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/add.html	2	351e541a80c6f2e0a05855c9d26105bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/edit.html	2	292df9274797759a37ce98788adab2bb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/left.html	1	22a172792822cc6b6656d63c7d1b8331
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/list.html	7	bb58b0bb4076bef88a5a2e4e103ba797
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/rename.html	2	7a9e40d904ce3b2952a5671e2642b6f9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/tree.html	1	8334d67e32801efc79b742d99df7547a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/resource/upload.html	2	40798f29575328f19d8efe43b9d46013
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/right.html	5	6d27fc989996a54fdd95b2e9bd436e6a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/role/add.html	2	7d6beee547650a732f4f8fb0a9976df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/role/edit.html	3	c7aaefbf9ab9c6171315935162ae6ec3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/role/list.html	2	b64703144d1b0e51b8877d2e7a791f40
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/role/perms.html	10	796145e2738f90418402002219c0c61f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/sensitivity/list.html	3	53b58cc56cc08baa17a3e125b8f102d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/site/add.html	4	178ea67cbd813f577cbcd4b661d70997
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/site/edit.html	5	bd168b8088577ef7035af23ad822cb3b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/site/list.html	3	847b9b2c1450d98dfbacc88c6eff3ceb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/site_config/base_edit.html	5	427934e4cde089abba0073db07d61b57
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/site_config/inc_opt.html	1	596fa716a29a1deeb63c5a4bc9f82da5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/static/channel.html	2	fb790ce8e0f0234c5eb7ead48ffe0c41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/static/content.html	2	54d348ff6ceea0bf118586de660dd932
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/static/index.html	2	1397f236f38f214df34207d39743eea7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/accessPage/list.html	2	482cf0d75251ba4c184caa0a22e34993
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/area/list.html	2	3077668c1af2690290950ee07cf0340c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/avgViews/list.html	1	395c2e6887c5300293b9ea933abc6df3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/comment/list.html	6	852296ea4ff658efaf5fdcb332a17db1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/content/list.html	6	124fb09c9e70cad12492c1b8ccddc199
/WebHallCMSV3.0BAProject/WebRoot/WEB-	6	22e965303f5d0c8f9e08c079856e922

INF/jeecms_sys/statistic/guestbook/list.html		f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/init.html	2	b19dfc5370f04c282486a4405a4fc2b3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/member/list.html	5	3161cecc6e3bf7213cb166bf1f4fc4e0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/pv/list.html	1	2363a3ed6bb791fd371414bb628809cf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/refererKeyword/list.html	2	d6564c392854e1829e3d9c48b03af1de
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/refererPage/list.html	2	09fa1ca03f4ffcf91eedc7502ef9e16c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/refererWebSite/list.html	2	a96dac6677902c7d8722f29a1997d1e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/uniqueIp/list.html	1	918c134fdeb10405a6e5148991d5bb34
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/statistic/uniqueVisitor/list.html	1	c51942620e34e9432090171c311f8d3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/tag/add.html	1	b6fd2cbd7693a56b05f250499b5f497e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/tag/edit.html	2	d3409321f6d8872edcd61dee15026c95
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/tag/list.html	3	dc72e52946f6cb673c933af115f732af
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/add.html	2	80b534561185ac9b253c16807587ae9c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/add_editor.html	2	56a14c1372dee7a11c894981b52e21d9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/add_textarea.html	2	1185bc4e962b095c41e3704ad1c6ef51
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/edit.html	2	2c85cf123ce442767633e8ebcf784b11
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/edit_editor.html	2	8eff70fb3ebc7c924a37a82467f4cd81
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/edit_textarea.html	3	f5f8b822de286f5f71b922412b98870c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/left.html	2	2b2f190f75001b8a894d605c36d77d21
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/list.html	6	99365c456754d6c31d9a257fd2f5e38f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/rename.html	2	826a299ddb9b00ef05d39bcdbd09cd80
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/setting.html	3	e5ce94b772891d5a1c5d9529512bd407
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/template/tree.html	1	657c03a4fe2eec13d8b09ea69b3bef26
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/top.html	9	f0341a5dd279156831da46af69acbd89
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/topic/add.html	5	fa8f66f64a0a7530d99f7d842fdc9999
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/topic/edit.html	6	624d396591a6a3c667fd23caffd000df
/WebHallCMSV3.0BAProject/WebRoot/WEB-	3	1a4cea2531f1087cae28362ae6de13d

INF/jeecms_sys/topic/list.html		f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/type/add.html	2	226918ef5c506d546678b08ba4df0c6c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/type/edit.html	2	3db9781a22e29606a1c6eb45d52b1a7c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/type/list.html	3	d5715c3e9367f291989b77429ee514f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/unified_user/add.html	2	951d7b288eb34e35b335d69e3c58c1db
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/unified_user/edit.html	2	7796a2a1b9d4e9a1bca4870c7ea4ba83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/unified_user/list.html	3	ff543a8488c82b92d9a8bb95e761829e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/vote_topic/add.html	5	066fd69d4d380f175dbcdb1852f22e90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/vote_topic/edit.html	5	1e277e73f1f7e0dde47de11bca64e14e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/jeecms_sys/vote_topic/list.html	3	6b47a4a76ddd15c1820c8f6bab8024de
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/fck/messages.properties	2	85625b26db7d5978542a2bffd6a641a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/fck/messages_zh_CN.properties	2	da70d06f0d16302a840df676e9dc4322
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_admin/messages.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_admin/messages_en_US.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_admin/messages_zh_CN.properties	47	b84ff082b60cfbabecda4fd5f47a8a81
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_front/messages.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_front/messages_en_US.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_front/messages_zh_CN.properties	2	d949c1cde9b9655bc8829025f63e0270
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_tpl/messages.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_tpl/messages_en_US.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecms_tpl/messages_zh_CN.properties	16	c8ecb7908ef74233154393ed33dfb706
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecore_admin/messages.properties	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-	1	d41d8cd98f00b204e9800998ecf8427

INF/languages/jeecore_admin/messages_en_US.properties		e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/languages/jeecore_admin/messages_zh_CN.properties	8	e6f8d423159ecce160cad8c53da171a9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/alone/╡Ñ╥│.html	4	6b516502f24baa8cbad959685c1ec7ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/═╝┐Γ└╕┬┐.html	7	8c19b1baf6f6db5dc81539f7ba6c95f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/═╝┐Γ└╕┬┐_╫╙╚╕┬┐.html	3	23b62604157b2a2760196d25fd9919f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╩╙╠╡└╕┬┐.html	8	d00f25a94fa3e94b056c5fca105660f1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╩╙╠╡└╕┬┐_╫╙╚╕┬┐.html	3	024677fb36a3bb91a0ba35230e57ba17
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╩┬╦╪└╕┬┐.html	9	fbf22a4a568b59a5fecd3af808c946f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╩┬╦╪└╕┬┐_╢■╝╢.html	5	4cd5c84bd1cd3b979dc56b3c5c5ca770
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_│ú╝√╣╨╠Γ.html	2	1acc45095f26db4349a9c7767e7c7b3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╕╕╝╢.html	5	3909d8ea0d667828b0aa4c8272d289fc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╕╕╝╢2.html	5	3909d8ea0d667828b0aa4c8272d289fc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╡ ¡╙¬─╔╒▒.html	7	0d8ae3907201b0753ad380a1f2b3e41f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╫╙╚╕┬┐.html	4	fd328fd43564a79fb48405b52486604f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╫╙╚╕┬┐2.html	3	ad72562b29862d781ecb413e266e206c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐_╫╙╚╕┬┐3.html	3	0ed15b5a3d6ee893459354ad77786a55
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╨┬╣╫┼└╕┬┐2.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╫≈╞╖└╕┬┐.html	4	ab774f9e9b2ce64a0f04b7eba150da84

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/╬≈╞╥└╕─┐_╬╙└╕─┐.html	4	74ebd09e7cad4bbe4276301715f4d2c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/channel/▒·╞╥└╕─┐.html	5	a4a90d2533009da81954188aeaf6572f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/comment/╞└┐▄╡▄└φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/comment/╬╥┤─╞└┐▄┴┴░φ.html	5	5b7a08226b819acaa7deada6c9c23d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/comment/▒Θ┐┤╞└┐▄╕╪┤.html	2	bfd9d532a970b6118bdbe745432ce404
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/common/│╒╣ª╠ß╨╙╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/common/┤φ╬≤╠ß╨╙╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/common/╥│├µ├╕╙╙╒╥┤╝.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/common/╨┼╧ó╠ß╨╙╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/═╝┐┌─┌▌.html	12	2c74fcc0835439d05a290021ddcd4619
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╨╙╞┤─┌▌.html	8	791566c038b15593bb1d6ebe69eb4e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╧┬ └╪─┌▌.html	9	5fe4a31d6274471580fd7bfa77c56327
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╨┌╬┼─┌▌.html	8	e26ca70d40d6cad2b72203c3f5251477
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╨┌╬┼─┌▌_│ú╝√╬╨╠Γ.html	5	e4d40dd1d9c200327c2e7e8404fee191
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╨┌╬┼─┌▌2.html	5	d6edcbb80a10eb493cbb656235e1e0ab
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╨┌╬┼─┌▌3.html	5	71a4fd40a942a9147de82e0db1cc2416
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/╬≈╞╥─┌▌.html	12	2c74fcc0835439d05a290021ddcd4619
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/▒·╞╥─┌▌.html	8	6fb43f02d4406dcc831c93229c51d529
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/inc_co	3	6cdd7ccfd9980fca3d628b7f26a342d3

mment_input.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/content/inc_comment_list.html	1	5ebf5dcd0403038a06f1c2e8f614f1a0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/csi/╖ß╘▒ ╟╥╝.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/csi/╞╘▀╙╙▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/csi/╣ת╕ µ.html	2	a9f92b7f8f5b888691632aafa2ad6e2a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/csi/╣ת╕ µ▒µ╣╗.html	3	ea07949812230fad9bc69eb92310d06c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/═°╒╡╡ ≈▓Θ╨ß╣√╥│.html	5	5206f8545de558f62530a125f413574e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/═°╒╡╡ ≈▓Θ╨Σ╚δ╥│.html	5	ae5f8b7d48a73b016aefb285e1db12ff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/ ╒■╞ ≤╕Ñ╢»╨╬╥│.html	11	3bebf64ac375d399b05f1fac095e1f97
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╓▒═ ¿│╡╨╬╥│.html	10	d368c299464bf7a4753b11b721178fd9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/┐ ╒╝ Σ╨╬╥│.html	29	47f011aaf17727ceee48ac3409474239
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╙├╕ º-╓ñ╒╒-╧Ω╟Θ.html	8	1de578374f6ffc5a45b7739aad6baa44
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╙├╕ º-╕╝╝■-╧Ω╟Θ.html	9	97a8e46b9859f850c01289d576592fd5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥ ╡╫¿╨⌠═°╥│╕ß╘▒╓╨╨═╥│.html	33	46c984214f2cfe721fa6cba744a37417
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥ ╡╫¿╨⌠═°╥│╕ß╘▒╞▄┬δ╨ ▌╡ ─╥│.html	4	65522aaea8502e50f4b8874085731eea
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥ ╡╫¿╨⌠═°╥│╕ß╘▒╨┤╧ó╨ ▌╡ ─╥│.html	16	f881476535991e27ae5f3f670fa0a909
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥ ╡╫¿╨⌠═°╥│╡ ╟┬╝╥│.html	4	4784f44753f81953abb5b60e55552857
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥ ╡╫¿╨⌠═°╥│╨╬╥│.html	28	1a59f78c1f626f0c98caa10de64b1380
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╞≤╥	32	0bd692cc49c0b93bfad6b5d8f50383f3

┤╫¿╩⌠═°╥│╩╢╥│-bak.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/ ╞≤╥ ┤╫¿╩⌠═°╥│╬╥┤ ─╫╩└╧┐ ┌╩╢╥│.html	29	06950eaac3e188e367ea96c99e369550
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ─╒╒▒╨┴╧ó.html	13	cd46c1e5642a8953d83cb5b76c6e2faf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╨├ ╞°╨┴╧ó.html	7	9a010fc51daed34ebb61002f76d0705e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╨├┤ ┬╨┴╧ó.html	7	681790b6b2633e547df2e712f139a177
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╨├╦«╨┴╧ó.html	7	a727bb9bdd4b35ecb037b696e204eeb4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ┤╪╒▒╨┴╧ó.html	7	c3a74b8eab266317b2e73408f5da0ea4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╣╪╫ó╨┴╧ó.html	5	7890aebae16fb2393ef9064834a082b4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╣·╦▒╨┴╧ó.html	7	6a218e9e172c77462abffc7e6bfad7ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╣╪╫ ó └╕ ╩╬╥│.html	15	79a3787ef7e9412bb14d4e0f4e2c5ca7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╬╥╥ ¬▒∞╩┬.html	56	33f17aa62a6cd8943b777dbe16333211
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/╬┐■ ▒╠ß╨╝Ω╠Θ╥│.html	4	b07ebbb5ef6655c280a542fa79260617
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/▒∞╩ ┬╠ⁿ╓┌┌≈╩┬╧ε└╨▒φ.html	17	f9a46609225ac74a5cc56cae6a970057
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/▒∞╩ ┬╠ⁿ╩┬╧ε└╨▒φ.html	20	4225dfc67d897f26b8becd32b2dfff8f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/▒∞╩ ┬╠ⁿ╩╬╥│.html	5	5aea6a27d4b6d88cf3e018231b8e89f8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/▒∞╩ ┬╠ⁿ╩╬╥│_bak.html	53	7137aa643c5f4e28f89a4a281ad39314
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/▒∞╩ ┬╠ⁿ▓┐ ├┼╩┬╧ε└╨▒φ.html	23	106c0371f0e77f5b248477e946253d9a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/back.html	9	2cc626d66193cc27beaec29a8639ee86
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/collection.html	9	c6c9bb97cef9a7ce81c10f73c820ffd1
/WebHallCMSV3.0BAProject/WebRoot/WEB-	11	77d5a758523a25658688b672225af7

INF/t/cms/www/blue_webhall/enterprise/complain.html		c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/consult.html	10	47d620ff182c9f10afe37ba686eff534
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/done.html	14	08a0f4b78161f56560d0fc7e13f4800a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/enterprise_iframe_upload.html	1	46e15af27f56320f486e406b11a9954b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/enterprise_image_area_select.html	6	6ce6585c98316444f18eee4f29dec7fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/enterprise_image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/image_upload.html	3	88a1665536f7d4fca03018ae1014bca1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/include/bottom.html	2	aaede3bf2fb5b683b41d72c5e756b253
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/include/indexbottom.html	2	71610baffcea4d97ccfd8b109524fa1b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/include/top.html	7	a7dc18dfb44bd1ecedd7f3df26bb08ca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/information.html	7	6fb7b11740ed91dbcb03185d01d2a025
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/online.html	8	0d9b0d5c51c3abef0906d5b4325d3b7b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/suggest.html	9	1eadf2c44cb1bf1498b62d303e537008
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/temporary.html	8	1158b080fe1c1ed8988c7dd900da6147
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprise/todo.html	8	7f0b1c7622a3e1104c54eb5dc912ad7b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╒■╞≤╕Ñ╢»╨╫╥│_gr.html	11	21475420e217f7c8ef95c09f03e280be
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╓▒═¿│╡╨╫╥│_gr.html	10	bb41e7ef52bfb9107bfe2cc09b799010
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╕÷╚╫¿╨⌠═°╥│╖ß╘▒╓╨╨─╥│_gr.html	26	887556a89ae452b456b7d06fbddc0c2e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╕÷╚╫¿╨⌠═°╥│╖ß╘▒├▄┬δ╨▐╡─╥│_gr.html	4	22661b13127093022468a239adbfe05f

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/ꟾ÷╚╬¿╨⌠═°╥|╗ß╚▒╨┴╧ó╨▐╕─╥|_gr.html	16	efef82a212202849e4783a6eec18434b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/ꟾ÷╚╬¿╨⌠═°╥|ꟾ╠┬╜╥|_gr.html	4	21ac04cb318a406cfa6764e11c5ffaa9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/ꟾ÷╚╬¿╨⌠═°╥|╨╠╥|_gr.html	26	4e4cec325c56bb95f6873552367bd257
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/ꟾ÷╚╬¿╨⌠═°╥|╣╠╥|_gr.html	19	623aa461f5dc8c470724aef7a97a1fc6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/ꟾ ╒╜Σ╣╠╥|_gr.html	29	30b00c4a9d204f1820c4a685c8dad286
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╙├╕º-╥ñ ╒╒-╧Ω╟Θ-ꟾ ÷╚╦.html	8	9eb508a9ee1a00e477e916b59b39c285
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╙├╕º-ꟾ╝╝■-╧Ω╟Θ-ꟾ ÷╚╦.html	9	4180e9c90537a45b82138928f1625495
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ─╔╔┴┴ó_gr.html	13	1b043080a3757e9edd4425ac6563e94f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╙├╞°╨┴╧ó_gr.html	7	ef31e534cd79763c7450b71eb6419792
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╙├┤т╨┴╧ó_gr.html	7	ef0844e5ca8831773f5b9b2f50904fea
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╙├╦«╨┴╧ó_gr.html	7	ce6bf9be898defe71b6875d960d4098a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ┤╪╔╔┴┴ó_gr.html	7	ec14501d5df14031db839d291c7e1f3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╣╪╬ó╨┴╧ó_gr.html	5	d35fea3a7173c2650e60eecc38787c53
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╣·╦╨┴╧ó_gr.html	7	54a375e5db659a71442a14bc6a024b98
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╣╪╬ó└ꟾ╨╬╥|_gr.html	15	89d7ca64c29156a84c9f2f49f88293a1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╬╥╥¬∞╨┬.html	55	711a5a73bad8395effe053242475916c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/╬┬▄╟╠ß╨╙ ╧Ω╟Θ╥|_gr.html	4	bb012d40246c37d3491568c877511ba8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/∞╨┬╟ⁿ╒╒╒≈╨┬╧ε┴╨φ_gr.html	17	b809bb5c31cd99e27f77277ac7b94b4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/	22	397aaa93aa9e9db44c360320eb2a45fe

∞╨┬╟ⁿ╨┬╧ε└╨▒φ_gr.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/▒∞╨┬╟ⁿ╨╫╥│_gr.html	5	12e2e84933254c0aa8e13926e2e037b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/▒∞╨┬╟ⁿ╨╫╥│_gr-bak.html	49	e2149df1b8d2cedbf62e8b0568e7e25b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/▒∞╨┬╟ⁿ▓┐├┼╨┬╧ε└╨▒φ_gr.html	24	a139bd9274c5b49b79083959a89f90a9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/back.html	9	cf47d31536572a33234fa9cecad25fe9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/collection.html	9	903d257352c41470cf7f87af0f3bc5ba
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/complain.html	11	0c7d2819417f0f00ef0e370fa33bb43e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/consult.html	10	6a95969c8636f1d79973019a913e81d9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/done.html	14	57b2d2964ed05ff78f1e174cd392584a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/enterprise_iframe_upload_gr.html	1	46e15af27f56320f486e406b11a9954b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/enterprise_image_area_select_gr.html	6	6bc812fb3819829df80effe1285ad226
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/enterprise_image_cuted_gr.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/image_upload_gr.html	3	99504710ced5e2e701d7115c50893fff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/include/bottom_gr.html	2	1c8cf47c44c16d1d5feda2b6a66dde70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/include/indexbottom_gr.html	2	d66aa4521073425e4285cd7c3e8115be
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/include/top_gr.html	7	d55fcba6a1d468bdb6ae729d266d56b4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/information.html	7	391c6756a35b86db066c077d8d06e76e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/online.html	8	94897a41e49ee66415faf3e246676b9d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/suggest.html	9	273ff16195f796582c356d4294769617
/WebHallCMSV3.0BAProject/WebRoot/WEB-	8	5904305c2ca65380c0539a4088eccee

INF/t/cms/www/blue_webhall/enterprisegr/temporary.html		3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/enterprisegr/todo.html	8	dd659b42d313aa141d69b9e39abbbcdd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/guestbook/┴⌠╤╙Ω╧┐.html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/guestbook/╬╥┤─┴⌠╤└┴▒φ.html	5	b4c8cab4ead68b5fe10f2193bcb30183
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/guestbook/▓Θ┐┤┴⌠╤╘╗╪┐┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/═╢╦▀┴┴▒φ╦│.html	5	807b88731525097a069995d36d6f4282
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/═╢╦▀╨Σ╚δ╦│.html	16	8f63df8413a5ab87aff8ee68cb321a76
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/═╢╦▀▓Θ┐┤╦│.html	4	79df1859b932fe9a97cfd20ee2c197f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/│í ▒╡╝╢╢.html	3	bea6601b1ea64201b7064802ac7a98f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╕Ñ╢»╜╕┴≈.html	2	b1a4368b661aaa507f636df4affaa54f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╕Ñ╢»╜╕┴≈_bak.html	2	e997574fa370bc3e73eb6f5410b28c03
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╜¿╔Φ╔╨.html	1	109c16ae4a8e659001541ae2e12ae35c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/├±╦┌╒≈╝»═│╝ ├┴┴▒φ.html	6	507ccf0c31da6929892dc3b392d5e455
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╢»┬▪┤≤╠ⁿ.html	2	7ce88e1403a12aaee0c1eb4835b876aa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╨╨_═╢╦▀╨Σ╚δ╦│.html	10	9931414d738bbb419aa3f4e7a05a9dbf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╨╨_╬╔╒»╨Σ╚δ╦│.html	8	341560b365beda4d694075daf72d2b40
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╬╔╒»┴┴▒φ╦│.html	5	236a6950b3ec4f82ad9f09f6b3c71626
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╬╔╒»╨Σ╚δ╦│.html	15	b3af2e639a8e1f5ab7aff3ae959bbe8b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/╬╔╒»▓Θ┐┤╦│.html	4	ae16444bc57f539f85d19f60d87e1704

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/20131209╕Ñ╢»╜╕┴≈_bak.html	3	daad22193bc1db88f6b87ba764a8acef
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/hdjl/android.html	2	826f51ebb373528c42229a3223549ec7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/═╢ ┣▒└╕.html	2	df2dcf97c712a39be416b301b085a0fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/ ╒■╬±╢½┐¬.html	1	364f5d48555fcca7d433270b810c2f44
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/ ╓ñ╒╒╒╧┤½┺÷╝╙╥│.html	7	33ef592d230b2837ac398f3cddeb5f9c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╕╜╝■╒╧┤½┺÷╝╙╥│.html	6	5ed0ba0f1fd56b4284ad0b049aa18f92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╡╝╟╜.html	2	6091055672 5a4c643695d7bb41274392
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╡╝╟╜1.html	2	f036c79572a2db09beb9e8e7a6a01a8b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╡ ╟┬╝.html	4	2dff4d8464ce1b397a33934b72ebec27
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╡╪═╝.html	4	c8bc45c5a70c04e846231f1d0d3e9c95
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╡╪═╝_zk.html	6	0b6841ea77044607187de486a8e925f8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╥│═╖╡╜╟╜└┐.html	2	cde19226de48cba19e1e42cdef5255bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╥│═╖╢Ñ└┐.html	1	0c274a91ce902366856f3cec846ad92b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╥│═╖╥╤╤≈└┐.html	1	329bbc3e0e514299d5a87e1ccd50b312
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╥│╜┼╨╕╟Θ└┤╜╨└┐.html	1	416d750f6bc37c48227ac5c673e30992
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╥│╜┼╨┼╧ó└┐.html	2	3e1f48cc4c523aefc1893b8a2e0e8037
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/┴≈│╟═╝.html	1	7f80229b68b4d648cf0281331f5a86aa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/╨┬╬┴╨▒φ.html	1	ccd0365feaae43b4bde644523d49f2bd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▒∞╝■.h	6	389c3e2e16ecf52cfaabf407de03a22d

tml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▒∞╝■_├┼╘┤.html	4	0389266b5f258e678a712dad44db34bb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▒∞╝■═|╝╞.html	2	a64f4e1a4d5b1818f362c1cc329a77b0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▒∞╝■═|╝╞╓╣╧╝ .html	3	fdf602e8b39152b97b1c73bb9fd0c6d1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▒∞╝■2.html	15	afc7ec04b2d40adb737722ddd703057e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/▓ó┴¬▒∞╝■═|╝╞.html	2	e1ebeecadadd38d7299b008a691a4b56
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom.html	4	b768c81a5f2f6f557b825a76433afe1f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom_╟╙╧.html	4	dfa69e83d01bca4e8e19ce0784ee9ac7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom_╟α╟ú╣í├┼┤╪╪.html	4	c31eb69b52d01178c844db917731ceb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom_▓╕╓¬.html	4	60a538d571d8e34b5321ce78461f4081
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom2.html	1	76d8d3846fea4761ad4e821b8e8a490d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom2_╟╙╧.html	2	b66657cbe6afd1bb09f7d95782884539
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottom2_▓╕╓¬.html	2	b078198eebf78489d95a13d8ae771da8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/bottomqzqd.html	1	065988aae0ebd020a1067068a7bcebbc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/clsc_box.html	12	53bba3460b78575bc6c29a57e85375c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/ditu.html	5	9d1ca0201f8247331e80d560b6609a9a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/form.html	4	6bcf07f9c39586a5f3c9de6fb4febf66
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/header_register.html	2	4cba08291225ba0ae8f690cb87601d79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/left.html	1	7291cfbed66834801368f6f05043cf68
/WebHallCMSV3.0BAProject/WebRoot/WEB-	1	a865c6c555cdb8d2f83467b4ae3dee5

INF/t/cms/www/blue_webhall/include/left_fuwu.html		b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/left_navigation.html	2	9e2d43ad4d50f43333696c4c17075d93
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/left_survey.html	1	161f04c62c84e24db06f6ebc9a80c472
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/left_zhengwugongkai.html	1	8b1a05713da1e75770d410631e66de6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/main.html	4	24af0e9ca33b56541b66a5d9196f195d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/menu.html	2	b96df307761e07850636c71c64d023ed
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/space_foot.html	1	290f37f47cfbbea16f824f618b57d012
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/space_top.html	2	3216313c32f4b9a7499062d3f7efd68b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top.html	10	29fdde6290dfe586fc60e9e28d0599ea
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_╟╚─╧.html	2	920adea87e8bc9dd612cc73d27333bc2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_╟╠α╟ú├┼┠┤╪╪.html	1	1517f08f8806e1a9a1113f6c4aae9e2c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_▓╕╔¬.html	6	d34007c98431ecc6484c4e03f9918f76
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_login.html	3	1ca8aa0b52579db863df86941c641d6c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_login_╟╠α╟ú├┼┠┤╪╪.html	4	40a25114e36d3fcbf8334bd884996944
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_login-▒┤╔▌ .html	5	c5937dc7cc68771d3bddcd4a80a06ae3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh1.html	9	6ce13012bdb1edff8ccc0957f4ccad03
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh2.html	9	606875a553a16b878f424e9faa0d4b30
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh4.html	9	518fb609adb54d023ab2f625902eac43
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh5.html	9	ba85d258fa3083775f6306310c8008b1

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh6.html	9	0700669a4389d6564438ffe9e3de2718
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top_xh7.html	9	dadb8c5f073987be1715ef406c687617
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top1.html	8	18772c5b223926b1f5a74bcb09b87ad7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top2.html	9	5bfd593d9c9bf6a39e04a2779c3a6c2b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top2_▒╕╓¬.html	6	826ea5d488b50b16cedc94273f43b761
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top3.html	6	d792c5cc14c3ab514813457a2d191216
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top4.html	6	b04d71726d09b8771eaecf885a69d4be
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/top5.html	2	e34ba11682c3c590282cb3fb15d91fcd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/include/topqzqd.html	2	9d28a09c2becabc2cd12eeafa549f21b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╒≥╝╓╥│├µ.html	71	ac04d7dd3a9999118d2ff9d662d25f99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│.html	15	206de9825b64bdf33098c7eb8a474bcf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│_╟α‖ú╝í├┼╒┤╪╡.html	22	2bfe5764023703e903f9d595cd932593
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│_▒╕╓¬.html	11	49e297b1e195799689e911a6b11620b4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│_hp.html	12	52cc721232471510d22f6fcf0233cf97
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│_zk.html	11	b807e7c5d1eeff5ca0ca931eb7ceceda
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│_zk_╕·╧╨═│╥╕.html	5	6b202116ed054b7ce161b1689ad1b9ba
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│2.html	89	5fa86f7492d59bbf5c486e358dbcbe8b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│2_╨┬╕ß_bak.html	36	dd57cd1ff24aa877a5d5a17b56005ba8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╧╠╥│2_╨	22	bc032302861d657919f95e5d7ff5a5e5

┬╧ε╖ ╓ └α╬┤ ┤ ╨╨²╛▌┐ Γ▒Θ╤».html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_▒╕ ╓¬.html	21	5e00b78eda7fc0820f335a5445621f40
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_1.html	4	57b8bcd01a9b25532881a6ada4ac8129
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_hp.html	22	9b8ae07865ee43d220cdc973b939c004
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_zk.html	19	d1c6dd272790e10cd296538fd1d89cb7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_zk_╕ ·╨╨═ǀ╥╗.html	41	37aea1f28d4919dd8a8fc6d6046aa3d0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2_zk_╨═¿ ╨├▒∞╨┬╓╕ ─┴▒µ▒╛ .html	32	e653b076dd9730ece58f666eacf88dbb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ2-▒╕ ╖▌ .html	15	4c4600c936e16860500ccd49036de773
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ3.html	5	5644b6ff0f7ea7eae11fb67ff3afdc8a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ4.html	7	047aafcd3d063a25c85787087aba8247
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ4╥┤ ╬±╧Ω╟Θ.html	4	0cdf6098009fbef1b955599f7637c168
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/╨╠╥ǀ5.html	89	5d1c2ae3df7a4841811ade7b18a72a15
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/index.html	8	0285cf10893ead3ee8903ac9c441ac10
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/index/index_jm.htm	10	ab98aa818d86c1b5e6e280019f498f98
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/ ╒≥╝ ╓ ╒╣╝╝ .html	8	5334c7fa0d22c52671313797074927 32
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/ ╒≥╝ ╓ ╝┬╧ε└╨▒φ.html	8	0c74c0a455e1fe70e51c3cdc62cffa3a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/ ╒Ω▒¿ _═Ω ǀ ╒╒Ω╟δ.html	7	f5d31eed17a7979851e64358b49920be
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/ ╒Ω▒¿ _╒┴┤ ½╕ ╝╝■.html	7	8684cc121e39a30bc0e15199a0482e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/ ╒Ω▒¿ _╒Ω╟δ╨º▒▄.html	5	d8a54f686615cdd81a5bac979af8956f
/WebHallCMSV3.0BAProject/WebRoot/WEB-	10	f6ac7cc651978bb7cb893fced0e4d52a

INF/t/cms/www/blue_webhall/lawguide/╔Ω▒¿_╠┘╝▪╬ ╙∞.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╔Ω▒¿_▒φ┤ Ñ╠ß╝╕.html	9	f9321d0ed683d6b011b0e68929b8826a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╝°╣ ╚▓Θ╤»╨┼╧ó.html	4	aa18afb5d601c2a84e24fd4385baa9c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╠°╕«╨┌╧ε└╨▒φ.html	11	9c5698b56a2f8c449f1bdbce78a94924
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╠°╕«▓┐ ├┼└╨▒φ.html	8	9ce531c780d874f6e01bd4502dfc0405
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╥┤╬±╧Ω╤╕ ╨┼╧ó.html	5	e0cdd9b216de5dcb150d637dfbe14e7b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╖╓└α└╨▒φ.html	4	ab571cbdfdd4424cd7878dc7d53f5e47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ.html	13	c7292b1c3ca1479f78b84c1c7ff0dc5c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_╝ ╔┤ └.html	10	49c1f35025212146d75c5121eee1b38b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_╝ ╔┤ └_1.html	14	c0dc4ef1fee53cb85e171f47dbfb391c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_╝ ╔┤ └_2.html	14	b9db2333ddd9bc2d908e4c9b7fd3861c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_╨ ╒├√.html	13	a79b1b16c6b14a4f228039794cbec691
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_╨ ╒├√_xh.html	9	f255281c806a8d9749263632167a07a8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_hn.html	10	4ff937dbe154a2fd1983bcd44fb00530
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_xh.html	11	bc76fba2b95a06c9d4e5d7438b82da97
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ_zk.html	10	82a6af9841019f28c6cc03f5d8d1b929
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ╨╡╧ε.html	14	5c59bb3bb9dfdf11f894676df1d74bd1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε└╨▒φ1.html	10	82aeb214d60165612fa2b504c9d66a9e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó.html	39	22824d74c831ac465d2ab60770774b36

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó_╣▄╧╨╖╣╬º.html	3	54ecfc13920049acb50938f2b02693cb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó_hn_╬ε‖≤▒µ▒╛ .html	27	3fc28016c6feebec08bc9c44de5551dc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó_zk.html	26	abeded636430185df71c09185edb2870
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó-▒╕╖▌ .html	13	c25e5ba003675cedd0f92c925632f875
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó-hn-4-12╖«╟▒µ▒╛ .html	28	1aa98bdd3f606bf330cdf52af313484c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╨┬╧ε▒φ╕ ±╧┬ └╪.html	6	15ebda62f69bb11beaed71a7e3efc8c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╬╔╦» ═╢╗▀╨┼╧ó.html	6	1d72a06889e24c858979b3c2fce363fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╣╦╦¬ ╞└╥Θ.html	7	6182a230b3e1a288fa37945a7f40043e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/╣╦╦¬ ▓Θ╤».html	4	379ea9e346a4a28b91541b396963c014
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/▓╖ ├┼ ╩╨▒φ.html	5	b85e041a58f5a1d78c08cf5ce79ee079
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/▓╖ ├┼ ╩╨▒φ_zk.html	5	db429fcddd7ae8bf47b1239c3ace275b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/▓╖ ├┼ ╩╨▒φ-▒╕╖▌ .html	3	dba7043116e74666a4f91de1fc1ca41a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/▒φ╖ ± ╩╨▒φ.html	10	4ec36503cacf03a684c50e11fa6cb5de
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/printcl.html	4	fecc515a46e258ec8f9d8dc2e8158bfe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/lawguide/wssb_matter.html	31	073a41dc5896066f815fde062e3aedcb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╕σ ╩╨▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╕σ ╨▐╕ ─╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╕σ ╨Σ╚δ╥│.html	7	7615a9f9f0461d731e3e10b249938184
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╦▀	6	c13ea8cb86ac7e8fb9a233709274a8d8

┴╨▒φ╥│.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╦▀╨▐┤─╥│.html	9	46aed1859838ccef2443f13dc9ebb276
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╦▀╧Σ╚δ╥│.html	9	cea3e992832c58654f2c710240f6dd94
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═╢╦▀▓Θ┐┤╥│.html	4	d3474ac940a2c9fb1c7a087b705efc73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═°╒╪≈▓Θ╨ß╣√╥│.html	5	6dadae57198d425742a71c689a27490f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═°╒╪≈▓Θ┴╨▒φ╥│.html	6	8bf120f5ef9f72582252cdecbaed0700
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/═°╒╪≈▓Θ╧Σ╚δ╥│.html	4	8812528f0649d559d5d5eb1acb1cfb99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ ╒╥╕╪├▄┬δ╨ß╣√╥│.html	3	9cc912c4946603f08451d598bfe133e0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ ╒╥╕╪├▄┬δ╧Σ╚δ╥│.html	4	5629c09b1c9ff567b5c085ff1581ba08
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒═╖╧±╨▐┤─╥│.html	4	7387641ee97790b8dbb38864747bd016
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│.html	6	417661d700b29b9aca802c9d4243db69
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╡╣╝╟╝.html	5	8bb34f2cbf3bb922f0a04577bb6f966d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╡╣╝╟╝_╟α╟ú╧í├┼╞┤╪╪.html	4	f21a2c2af1d7ac27c1b50ade3ac0a1dc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╥│═╖.html	2	18333b28668e1999b4d9f6625e259a5d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╥│═╖-▒╕╖▌.html	2	f59bb4939910f762b151e51b37329110
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╥│╝┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╔╨─╥│_╥│╢Ñ.html	1	83b2c77379ee566bb216a550b8a51df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒├▄┬δ╨▐┤─╥│.html	4	b5584694fdb85e37a97e15a2f6ec4f8a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß╚▒╡ ╟┬╩╝╥│.html	27	f649b4fad5b5c3655dd79be782d54722
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	72e9452902af26c5ee8bb4ab455b05

INF/t/cms/www/blue_webhall/member/╕ß┖▒ ╡╟┬╝╥│_▓╕╓¬.html		50
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß┖▒ ╤Θ╓ñ╨┴≐ó╨▌╡ ─╥│.html	12	0b400ad7c936d39e6a1acf8a7aeea0b1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß┖▒ ╨┴≐ó╨▌╡ ─╥│.html	18	535ab61861c3a82d0f3be460d7c25f05
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß┖▒ ╫ó▓ß╥│.html	48	d61617bdf0ab2829d5af4f9168a3a03b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╕ß┖▒ ╫ó▓ß╥│_zk.html	19	d4dd6eae40e5f36249e38a6d98867a6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╙╨╓ñ │╒╢ª╥│.html	4	262def1248b947af8c4ba9a46db7d7fd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/└╧╙├ ╕º░≤╢¿╜ß╣√╥│.html	3	83e7dd821ee8ab95793d9f912ab9da91
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/└╧╙├ ╕º░≤╢¿╥│.html	4	5629c09b1c9ff567b5c085ff1581ba08
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ └ñ╙ ─╒▌╥│.html	4	ef17a8ff5c7fee72b7906441da7ce2f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ └ñ╙ ╧╨░φ╥│.html	6	f438c6184e03b6197071fd6e71d3a7d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ └ñ╙ ╨Σ╙δ╥│.html	9	56d00a47457aa5cf4be498d10e3592d7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ └ñ╙ ╨Σ╙δ╥│2.html	7	6f3cade0051808d3c61673505f215ade
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╜º╢ ╙▓ Θ╤»╨┴≐ó_╕ß┖▒╓╨╨─.html	4	334c0bad59770dbd061007fd3398e9c2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╜ñ╕ε│ ╒╢ª╥│.html	4	e988ec59cbe93ef9159c2cfa2b13e55c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/ ├■┬δ╓ ╪╓├╥│.html	2	9a323cd231b7e8bb229fa04eed9430c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╡ ╟╞╜ ╫┤ ╟¼╥│.html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╡ Ñ┤ ╓ ╡ ╟╞╜╡ ▄╡ °╥│ ├µ.html	1	86cf8b55270eae9485b526ed0c44b6c5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╨ ╒▓╪ ╨┴≐ó╨▌╡ ─╥│.html	5	a00123423e284e96db5d8aea5954deeb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╨┬╙├ ╕º░≤╢¿╜ß╣√╥│.html	2	154ef81ee69e8403e77060135cef872f

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╨┬╨├╕º▒≤╢¿╥│.html	6	650e7e974d8f6e6f6be966948d97844b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╫╔╥»┴╨▒φ╥│.html	6	ddfbd7a98eb68aee52a8ec15ca430ff4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╫╔╥»╨▐╡─╥│.html	7	c793d1193a7dcff30a75869e8351eff2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╫╔╥»╨Σ╚δ╥│.html	8	061d48678b4eeb8a38d0a80570404bd7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╫╔╥»▓Θ┐┤╥│.html	3	6a772e73af1b87b98ced25bfecd73866
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/╫ó▓ß╝ß╡√╥│.html	4	1ea3c248bcf408e577bf197f36fbf440
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/CA╗ß╘▒╫ó▓ß╝ß╡√╥│├µ.html	1	ee3070c1757cccb8491a24a14725a86a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/CA╗ß╘▒╫ó▓ß╥│.html	26	54cd023dd8c5fe0dd64f156913be1a38
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/mobileGetClInfo.html	14	669ae1d605a2b7311b6767637db8f0dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/member/mobileSaveClInfo.html	1	38370d102c36090aeb9d757fa0d92079
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/ ╞╛─┌╨╪╣▄└φ╥│.html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╗╪╕┤╥│.html	4	4a99ed086e3e9b7ade428de35265c225
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╖ó╝■╧Σ.html	4	8e1b3bdb8c33f3a196f90b008accf3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╖ó╨╪╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/ └¼╗°	4	4cc580ef4385f28cd6957a10e871d028

╧Σ.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╨╒■╧Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╨┼╧ó╘╟┴╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/╨▐╕─╨┼╧ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/message/▓╕σ╧Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/opinionrecord/├±╥┌╒≈╝»_╧Ω╧╡.html	3	d7ddbc393fab7926360d0c1427bae862
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/opinionrecord/├±╥┌╒≈╝»═│╝╞.html	5	49b2bfef71e633d20ad3fa842b0c9995
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/opinionrecord/├±╥┌╒≈╝»└╨▒φ_╕÷╚╦.html	5	215d998f5fbb95995ba04178e54d8a69
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/opinionrecord/╥┌╝√╨Σ╚δ╥│.html	5	b1425f8cf43f903b3d9715faa27e42e1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╟σ┤Ñ.html	5	ff3aa155962c2316f86fdc6a3537dcc0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╟σ┤Ñ╚¿╘≡.html	11	8b776dc4927c473f5cde6ebb175d0be1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╟σ┤Ñ▓┐├┼.html	10	1e7ef7295e0507b9705bc0d72e2c7fd4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╥╟╨╨╒■╨φ┐╔.html	5	f55b780033f55fb3d4eaba2f25ed84bf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╞Σ╦ⁿ.html	4	1cd90e9a9829b34683f14f2d7ec694e6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╨╨╒■╒≈╨╒.html	4	6b569cf18f2dcf638f4a17a2eded4560
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╨╨╒■╖╕╝.html	4	2b4e383a69e3e985f06be59395e87a9e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╨╨╒■°╕╢.html	4	949ae481487292dcd63c240deadc1fa3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╨╨╒■╚╖╘╨.html	4	ce0fcd02ce72fb4eb9f802123d9aa686
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿╘≡╧Ω╟Θ╨╨╒■╝∞▒Θ.html	4	3e59f98a6e924291c307dd396f06ecee
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	f1cef5f48f327d0ef732f86227dd7556

INF/t/cms/www/blue_webhall/qzqd/╚¿ ╘≡╧Ω╠Θ╨╨ ╒■╠┐ ╓╞.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿ ╘≡╧Ω╠Θ╨╨ ╒■┤ª╖ú.html	4	ee0a7dbe4ff6c42f5f3988212dd3a5f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿ ╘≡╧Ω╠Θ╨╨ ╒■╨φ┐ ╓.html	5	40f8539cd51d0ff12d18ade8ab6fa3c2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/╚¿ ╘≡╧Ω╠Θ╨╨ ╒■▓╞╡ ÷.html	4	b8cae6d1e211d980082ec8a2d3bf2de1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/2╝╣- ╚¿ ╘≡.html	9	5b4161374fb4179b8e24a9450f51f3a7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/2╝╣- ▓┐ ├┼.html	6	20eefa7da13f3893fcbfcd18280a43d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/3╝╣- ╧Ω╤┐ ╨┤╧ó.html	6	9bd1461af51dc4817775746f63f24c22
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/qzqd/main.html	8	ab8a16d186ec3d6b912596aa67294958
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/show/═° ╒┘ ┤╪═ ╝.html	3	694c5c062e37db068953f60bc8a02a96
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/show/╨╣╢ ╙├▒∩╓ ·.html	3	57d47fedabada2b86eb3d62c5e71862b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/show/┴¬╤┤╬╥ ├╠.html	3	c526e877a05399df809dfac37bd57514
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╓ñ╒╒╒╧ ┤½╥│.html	7	9284bc81288d77a98baafece61886f70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╓ñ╒╒└·╨ ╖▓─┴╧╥│.html	8	e05be171af80d3206f379619c12fddf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╓ñ╒╒╨┴ ╧ó╥│.html	6	ad55fd77dc576498e6c1918996631f54
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╕ ÷ ╚╓╨┴ ╧ó╥│.html	13	718746e5bfd8a0ef0234a69de0399553
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╕╨╝■╓╧ ┤½╥│.html	7	b13c01aff4b81b419ebf2425299ca5ca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╕╨╝■└·╨ ╖▓─┴╧╥│.html	7	48bb6389e72a003a23d1e5fcf7913add
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/╕╨╝■╨┴ ╧ó╥│.html	6	84cf8291515a30d5c781634a46d68122
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/ └·╨╖▒∞ ╝■╥│.html	6	310c9efbd5de4e177f680b9c53d7f483
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	0f7f6f8cfdb83cc67cf4374d2d9ebb3a

INF/t/cms/www/blue_webhall/space/ᅻ ╟┬┛╥│.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/clsc_box.html	9	70126b998d366011e4d01975984070ff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/main.html	4	24af0e9ca33b56541b66a5d9196f195d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space/menu.html	2	b96df307761e07850636c71c64d023ed
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╥ñ╒╒╔≒┤½ᄂ÷┛╙╥│.html	7	f27500fb62571ef9e134ee0cc4c23191
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╥ñ╒╒╔≒┤½╥│.html	7	9284bc81288d77a98baafece61886f70
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╥ñ╒╒└·╨╖▒╼┴≒╥│.html	8	e05be171af80d3206f379619c12fddf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╥ñ╒╒╨┼≒ó╥│.html	6	ad55fd77dc576498e6c1918996631f54
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ᅻ ÷ ╙╦╨┼≒ó╥│.html	13	718746e5bfd8a0ef0234a69de0399553
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ᅻ ╨╜■╒≒┤½ᄂ÷┛╙╥│.html	6	5ed0ba0f1fd56b4284ad0b049aa18f92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ᅻ ╨╜■╒≒┤½╥│.html	7	b13c01aff4b81b419ebf2425299ca5ca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ᅻ ╨╜■└·╨╖▒╼┴≒╥│.html	7	48bb6389e72a003a23d1e5fcf7913add
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ᅻ ╨╜■╨┼≒ó╥│.html	6	84cf8291515a30d5c781634a46d68122
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╨├╕º-╥ñ╒╒-≟Ω╟Θ.html	9	fe608ab0f27f20ecd22fd4bbf296001a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╨├╕º-╥ñ╒╒-≟Ω╟Θ-ᅻ ÷ ╙╦.html	9	616ab53bedca1a2bb32920812dededed28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╨├╕º-ᅻ ╨╜■-≟Ω╟Θ.html	9	97a8e46b9859f850c01289d576592fd5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/╨├╕º-ᅻ ╨╜■-≟Ω╟Θ-ᅻ ÷ ╙╦.html	9	4180e9c90537a45b82138928f1625495
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ └·╨╖▒∞╜■╥│.html	6	310c9efbd5de4e177f680b9c53d7f483
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/ ╞≤╥┤-ᅻ ╨╜■-╔╛ │².html	3	72c2e46031b63b432358faa6cea91525

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/clsc_box.html	9	70126b998d366011e4d01975984070ff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/main.html	4	24af0e9ca33b56541b66a5d9196f195d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/space2/menu.html	2	b96df307761e07850636c71c64d023ed
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/═╢ ╞▒╨ß╣√╥│.html	5	e0d54717779ab10191cfd26d1dabcc41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/═╢ ╞▒╟ß╨╕╥│.html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/═╢ ╞▒┴╨▒φ╥│.html	6	41365dc9c22bd1edd702151c1f9a2cbd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/═╢ ╞▒╩Σ╚δ╥│.html	4	ce21030202144bc723a95d9922b41b2d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/ ╞└┬▀╥ │.html	5	9cc103a15fbf86703a80bbba038cc44e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/╥╥╥≈╨ß╣√╥│.html	4	440206ac7b548aba2c485bc01a5ea72a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/╥╥╥≈╨ß╣√╥│2.html	3	5b5c9e5d4b61f774f04316b745278c4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/╥╥╥≈╩Σ╚δ╥│.html	4	c9a57c42388a726696d743843f241bfa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/┴⌠╤╘▒σ└α▒≡╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/┴⌠╤╘▒σ╩╬╥│.html	12	9fc6b6bf9a26f917c001068665fb9321
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/┴⌠╤╘▒σ╧Ω╟Θ╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/▒Ω╟╒╡╝ ╟╨╥│.html	3	e7af22f78671b6f6299bf98066f0d1f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/▒Ω╟╒╧Ω╟Θ╥│.html	4	86026c490e51002735d430b046d7e3ce
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/style_page/cont	1	0083887e27c572e0b7a4d553978d330e

ent.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/sync/╨²╛▌═¼▒╨╨┬ └÷╥│.html	3	a8276a6242204381996d1db55120d880
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/sync/╨²╛▌═¼▒╨┴╨▒φ╥│.html	6	aff734a64ab44ba1a0368b6dfce99947
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/sync/╨²╛▌═¼▒╨▒α╝ i╥│.html	3	a0c22cc8b94148c7dfca25c81e110fb9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/topic/╫┐╠Γ─¼╚╧╥│.html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/topic/╫┐╠Γ┤╣╢╣╥│.html	3	8bcdb098db1d13d1a17cf150ace074b4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzsp/═╢╫╧╔≤┼·.html	12	e31fb5bf7a7652704e8b6da5d75429ff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzsp/═╢╫╧╔≤┼·1.html	7	07c2ea72e9733ff5d30f254c63d72870
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzsp/═╢╫╧╔≤┼·2.html	11	f10f270fadab03fc0b291de2546894c8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzsp/═╢╫╧╔≤┼·3.html	8	828401aed2f3081bd738a14179eee3c5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzspba/═╢╫╧╔≤┼·.html	18	f69068bb17618b7371e70450f39d6299
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzspba/═╢╫╧╔≤┼·1.html	24	3b1804508729f35ca263691247d37c4d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzspba/═╢╫╧╔≤┼·2.html	29	980c99fd0b2035a6f30cf43ffe71dc4f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/tzspba/═╢╫╧╔≤┼·3.html	26	418ecbb3554350b11656acd977fec425
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/banjiejianlist.html	17	6483f3f2b28fae2479243a9d978cef35
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	a9578dbd7f290ac074f7340fc00cfdff

INF/t/cms/www/blue_webhall/wssb/busiindexlist.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/businesscouncillist.html	6	2b7a50ecac53c6e4f1d5e3ab6d0b9f90
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/busizxfwlist.html	2	d8e8d8e3ba9de8b2a1596d690537ddcc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matter.html	13	6aee1c63b58cf90917e37e8155c1043c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matterdetail.html	11	33205e0da1099c5a6ab7fd17eea5833c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matteredit.html	15	d2b39b95dc93767f1e621f7b2979ff67
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matterhtml.html	57	8630bc4ddb92fb18559ba9271e850866
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matterhtmlbak.html	35	9443c4e3871ad5ae737a156a805fc71a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matterhtmledit.html	68	e7f9c6200e24c259d2f3aafea57a380e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/matterhtmlshow.html	34	c862b84b23fb9547331e35825b1b9cc1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/tuihuijianlist.html	10	796eff380b447a3cd004aa261bd94658
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_download.html	5	44c20cbe5b1834abafdd6c23a6404e98
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_lawguide.html	26	ee530bd32e4dfbc280df931748aa05e0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_lawguide_hn.html	28	04c931d7b8d1b82e50634c0f9d63abb4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_lawguide_zk.html	26	1d2eb9217a10a774a8b61d525c423b1e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_lawguide-▒ㄱㄲ▌.html	12	31bc6d9ca75e7c6c808786f67aa19cd0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_permbysort.html	10	dc66e36847190ebb5a7c51084cd67342
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssb_permissionitemsort.html	5	cc907dd46257da446081abe456d5535b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbdeptlist.html	4	1371862aa2890d1aa3fe6c6eff4a0010

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbdeptlist-▒╕╖▌.html	3	83261f2e512e0f4989a8f3becbd6ea7c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbpermlist.html	13	92306f3c394a279c2a02be5430baaa5f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbpermlist_hn.html	11	e63cc38e8919c536d5d2bf128ac46c2b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbpermlist_name.html	10	d41bf554cc6a517344e33d06398199c8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/wssbregiondeptlist.html	7	aebb47377c637c29d81310bbd53cd4bd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/zaibanjianlist.html	12	1714cb5a1ccb2bb6607bd778a043c9e6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/wssb/zancunjianlist.html	9	8b145c83b78cdeb97a047727275d4e6e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/ ╒■╬±╣½╖¬.html	8	10fcad3866d8d2373b0ecf324c55b834
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞.html	8	e6c9160e15139adfbf02028d503fe326
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞-╓┘Γ².html	45	971495cfbb5b9533cb1834963fc254e1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞1.html	24	14e0437c1abca791e3ed5de6659f4101
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞1-╓┘Γ².html	45	0fcdf9f78d076c01e3c704ab02eb0f92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞2.html	11	7da5f595aa38372ee0d024c645c70865
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/xnjc/╨º─▄╝ɑ▒∞3.html	6	38090819c1002879cfd3523e7e162261
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zcy/╞≤╥┤╨°╢╚▒Θ╤».html	4	577dd437bd2259e5037c331fefb9c0ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zcy/╞≤╥┤├√│╞▒Θ╤».html	6	0afa365920b05357d61abdc974f1eb64
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zcy/╞≤╥┤┤╟╣╟.html	5	17de10072af07ec6eac18d651fc13495
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zcy/╞≤╥┤╫ó▒ß.html	11	8cee88abe14809499b0f68c509406a63
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zcy/╫╓╟┼▒Θ╓╪	7	ccd46eb6320ff5f7cf3240ed6266e917

.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/ ┌■╬±╣½┐¬.html	22	6871c7d6ab236b02fe0b363cbe2768d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/ ┌■╬±╣½┐¬_▒∞╨┬╥└┘▌.html	20	b19bb595c5cb59bee69724c8a06386f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/ ┌■╬±╣½┐¬_▒∞╨┬╥└┘▌_▓Θ╤».html	24	4715c60d5b2b8445ce671be6738d50e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/ ┌■╬±╣½┐¬╣┬╧ε╨┼╧ó.html	14	5965ca30e069252f76f92354d7632393
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/tzga.html	6	913782cf4764bb5781ccfced3ac9d68e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_webhall/zwgk/tzgaitem.html	7	d7133a9fd23c7fd387e29c600ec538d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/alone/┤Ñ╤│.html	4	a1eae4664683512818bb650a45e404bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/═╝┐┌└┤─┐.html	7	8c19b1baf6f6db5dc81539f7ba6c95f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/═╝┐┌└┤─┐_╫╙└┤─┐.html	3	23b62604157b2a2760196d25fd9919f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨╙╞╡└┤─┐.html	8	d00f25a94fa3e94b056c5fca105660f1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨╙╞╡└┤─┐_╫╙└┤─┐.html	3	024677fb36a3bb91a0ba35230e57ba17
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╧┬╘╪└┤─┐.html	9	fbf22a4a568b59a5fecd3af808c946f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╧┬╘╪└┤─┐_╢■╝╢.html	5	e151308e16ca8602c443f9896f9892c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐_╕╕╝╢.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐_╕╕╝╢2.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐_╫╙└┤─┐.html	4	1af4459bb6e40768970e70313e300570
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐_╫╙└┤─┐2.html	6	05f0a6c896c8fa5b95aa96cc634a41e5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╨┌╣╪└┤─┐	12	2c3a2a4bece5488832c2c003905c3a3d

╕─┐2.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╬≈╞╖└╕─┐.html	4	ab774f9e9b2ce64a0f04b7eba150da84
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/╬≈╞╖└╕─┐_╬╙└╕─┐.html	4	74ebd09e7cad4bbe4276301715f4d2c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/channel/▓·╞╖└╕─┐.html	5	a4a90d2533009da81954188aeaf6572f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/comment/╞└┬╣▄└φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/comment/╬╥┤─╞└┬▄╨▒φ.html	5	5b7a08226b819acaa7deada6c9c23d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/comment/▓Θ┐┤╞└┬▄╗╪┤.html	2	bfd9d532a970b6118bdbe745432ce404
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/common/│╒╣ª╠ß╨╙╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/common/┤φ╬≤╠ß╨╙╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/common/╥│├µ├╕╙╙┌╥┤╜.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/common/╨┴╧ó╠ß╨╙╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/═╝┐┌─┌╢.html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/╨╙╞┤─┌╢.html	8	791566c038b15593bb1d6ebe69eb4e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/╩┬╘╬─┌╢.html	9	7af83f7dab3e0d0e6723d456477199e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/╨┐╬┤─┌╢.html	8	e26ca70d40d6cad2b72203c3f5251477
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/╨┐╬┤─┌╢2.html	8	9794f9db12a8a72a1bd2c31d7abb6e81
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/╬≈╞╖─┌╢.html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/▓·╞╖─┌╢.html	8	6fb43f02d4406dcc831c93229c51d529
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/content/inc_comment_input.html	3	6cdd7ccfd9980fca3d628b7f26a342d3
/WebHallCMSV3.0BAProject/WebRoot/WEB-	1	5ebf5dcd0403038a06f1c2e8f614f1a0

INF/t/cms/www/blue_website/content/inc_comment_list.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/csi/╗ß╘╡╟╦┘.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/csi/╞└┬┴┴▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/csi/╣∩╕µ.html	2	a9f92b7f8f5b888691632aafa2ad6e2a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/csi/╣∩╕µ▒µ╬╗.html	3	ea07949812230fad9bc69eb92310d06c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/guestbook/┴⌠╤╘═Ω═╕.html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/guestbook/╬╥╡─┴⌠╤┬┴┴▒φ.html	5	b4c8cab4ead68b5fe10f2193bcb30183
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/guestbook/▓Θ┐┤┴⌠╤╓╣╪┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/═╢╤▀┴┴▒φ╥│.html	8	28d1087e574a64a403fd77a0500de807
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/═╢╤▀╨Σ╙δ╥│.html	13	64f96a33d536bfce7862555da1fcf269
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/═╢╤▀▓Θ┐┤╥│.html	8	30c9c7a4c278129ee2bc6b7774bb6737
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/╖Ñ╢»╝╖┴≈.html	2	360d8dc1e17a390445a798d04a639ceb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/├±╥┌┌≈╝»═│╝╞┴┴▒φ.html	5	d0ae5c5cda2bb935727a2a35ecaff043
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/╫╒╤»┴┴▒φ╥│.html	8	8cbde9bc775e8a12b20f9a6339eee1b5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/╫╒╤»╨Σ╙δ╥│.html	11	0620ed2f71ebf1fae6b4803f37a848f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/hdjl/╫╒╤»▓Θ┐┤╥│.html	7	ba427be2859a5d324264ceb13f0ff03d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/═╢ ╞▒└╕.html	2	1aa8f3f08d07a4683a9fc3b06203f3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/╡ ╟╦┘.html	2	83a535bdab827d319497bee72f3d4bca
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	cde19226de48cba19e1e42cdef5255b

INF/t/cms/www/blue_website/include/╥│═╖┤╝╢╝└┐.html		c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/╥│═╖╟Ñ└┐.html	1	0c274a91ce902366856f3cec846ad92b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/╥│═╖╥╤╤≈└┐.html	1	329bbc3e0e514299d5a87e1ccd50b312
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/╥│╝┼╙╤╟Θ└┤╝╙└┐.html	1	416d750f6bc37c48227ac5c673e30992
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/╥│╝┼╨┼╧ó└┐.html	2	3e1f48cc4c523aefc1893b8a2e0e8037
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/▒∞╝■.html	4	9b989fa97733ef17cb0598c8e8b652e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/bottom.html	3	521c1607dece28a9ef2e353edac99341
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/header_register.html	2	4cba08291225ba0ae8f690cb87601d79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/top.html	6	1a38b37327f7684f58cff82e6945fbd9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/include/top_╧╠▒▓.html	6	b60871f42a660236d7388aeb99b93c7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/index/╨╬╥│.html	16	3220f4f4b4b101a6b2f7dbc6090fa70c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/index/╨╬╥│_╧╠▒▓.html	14	330e2c260ba1e52f9f3f613d4c86a78d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╠°╕«▓┐├┼└┴▒φ.html	6	1a660269725e02a510b86ac7d749b830
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╥┤╬±╧Ω╤╣╨┼╧ó.html	6	e5f29a35d1dd7b0b5e70ae3e1fe87abd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╨┬╧ε└┴▒φ.html	8	5468434c6b782b6d9a5b8adae0d0c0de
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╨┬╧ε╧Ω╤╣╨┼╧ó.html	7	e5942905f44981bed183686ad7023a10
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╨┬╧ε▒φ┐ ±╤┬ ╞╪.html	7	08695a7b9e1b4b8ab3ec868df19dc26d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/╪╔╥»═╢╓■╨┼╧ó.html	6	26957be4c882aac7d1cb53fc65a89e4e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/lawguide/▓┐├┼└┴▒φ.html	6	c63a26750d209734a1fc9e760ccdb686

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╕σ┴╙▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╕σ╨▌╡─╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╕σ╩Σ╚δ╥│.html	7	7615a9f9f0461d731e3e10b249938184
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╤▀┴╙▒φ╥│.html	5	cc6af55eae463cdb261066a1372568f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╤▀╨▌╡─╥│.html	5	d75ef87e25b61dd94380a4a63301f7f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╤▀╩Σ╚δ╥│.html	6	6270ce29c9f41f18cc8fbf1a2090102e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/═╢╤▀▓Θ┐┤╥│.html	4	679858f3cb5b2685e5cde712247ced75
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ ╒╥╕╪├▄┬δ╨ß╣√╥│.html	4	8119a749811cd6788cfc33ab7df8e5f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ ╒╥╕╪├▄┬δ╩Σ╚δ╥│.html	6	89d0459446b68c36dc86ccbe0ee3a86c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚═╨±╨▌╡─╥│.html	4	7387641ee97790b8dbb38864747bd016
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╒╨╨┘╥│.html	9	591ffb688fd1d649747cf21a6a66496e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╒╨╨┘╥│_┤╝╢╜.html	3	60daf5af520a2a25a42b3888f9390b10
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╒╨╨┘╥│_╥│═╖.html	1	e06c1338783b1ba5230b5ce95f9a9b7d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╒╨╨┘╥│_╥│╝┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╒╨╨┘╥│_╥│╢Ñ.html	1	83b2c77379ee566bb216a550b8a51df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚├▄┬δ╨▌╡─╥│.html	3	b731e1f96d6f2188035b0795fbf19240
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╡┤╡╝╥│.html	6	2c13a6e45664cdb43d768f46dcf7cf6a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚╨┼┴ó╨▌╡─╥│.html	13	c68cbb326ea9148ba1ba3aaf998a1a1f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╕ß╚	18	c2c81af9c81aadbe87342877ed620fb4

╫ó▒ß╥ | .html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ ╘ñ ╙ ╨╨▒φ╥ | .html	5	ae33e2ee421ed0d3057d372c629a732a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ ╘ñ ╙ ╩Σ ╚δ╥ | .html	8	022b908c73aec834dc2d0734c44c6852
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ ╘ñ ╙ ╩Σ ╚δ╥ | 2.html	7	6f3cade0051808d3c61673505f215ade
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╜ñ╖ε | ╒╣ª╥ | .html	4	3ca6cbbf4cfbda0da62d7a29fd04281e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ |▄┬δ╓ ╪╓ |╥ | .html	4	eb2a01069b666f590f6f7ee2153e5f6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/ϡ ╠┬╝ ╬┤ ╠¼╥ | .html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╨ ╒▓╪ ╨╨▒φ╥ | .html	5	a00123423e284e96db5d8aea5954deeb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╫ ╒┬» ╨╨▒φ╥ | .html	5	a82ec5213adbce3ec05052460ee3b082
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╫ ╒┬» ╨ ▌╡ —╥ | .html	4	5d0a31733a44c51e4395e6329ef9b739
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╫ ╒┬» ╩Σ ╚δ╥ | .html	4	013f6a8ba88bb8a8e399a520d798f40f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╫ ╒┬» ▒Θ┐ ┤╥ | .html	3	57d04681bc76b92f966293b33ef04745
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/╫ó▒ß╝ ß╣ √╥ | .html	4	407aa6d23b7ad235e20c1fd72c85b8d9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/ ╒┘ ─┌ ╨┼ℓ▄ └φ╥ | .html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/╖╪╕┤ ╥ | .html	4	4a99ed086e3e9b7ade428de35265c225
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	8e1b3bdb8c33f3a196f90b008accf3f7

INF/t/cms/www/blue_website/message/╖ó╝■≚Σ.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/╖ó╨┼╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/└¼╕°≚Σ.html	4	4cc580ef4385f28cd6957a10e871d028
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/╨╒■≚Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/╨┼≚ó└╢└╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/╨▌╡─╨┼≚ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/message/▓ ╕σ≚Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/═╢ ╞╨ß╣√╥│.html	5	d982ee772b37dcc69ce0163a764aea87
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/═╢ ╞╨╟ß╨╕╥│.html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/═╢ ╞╨╙Σ└δ╥│.html	1	3df0cbfd78067fc65548fd492b13385b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/ ╞└┬▌╥ │.html	5	be843242d7a1d606576de28d1892cc28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/╥┬┬╥≈╨ß╣√╥│.html	4	decc1f8c3d4519857d65d3263169f48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/╥┬┬╥≈╨ß╣√╥│2.html	6	a826266770fa90f30cdc09562f83cde9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/╥┬┬╥≈╩Σ└δ╥│.html	4	b9c6784384d78a7d45cd653c152125f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/┴⌠╤└▒σ└α▒≡╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/┴⌠╤└▒σ╦╬╥│.html	12	033f978b50f64e84ab229ca0c96a9b73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/┴⌠╤└▒σ≚Ω╠Θ╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/▒Ω╠┌┤╝ ╠╩╥│.html	3	fdeaa32873e1a172e6ef73ca22a92913
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/▒Ω╠┌┴Ω╠Θ╥│.html	4	3f905c5ddea0680e6c36d40ba72ef786

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/style_page/content.html	1	0083887e27c572e0b7a4d553978d330e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/topic/╫┐╠Г─¼╚╧╥│.html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/topic/╫┐╠Г┤╝╟╝╥│.html	3	327dfb80de1d22dba5b06dc47ae7b6f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/banjiejianlist.html	7	e0bdbc03359d29d9d4bcda388b9e2103
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/busiindexlist.html	2	a9578dbd7f290ac074f7340fc00cfdff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/busizxfwlist.html	2	d8e8d8e3ba9de8b2a1596d690537ddcc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/matter.html	10	ea7ce199ebc98584ac5f06819dcff12e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/matteredit.html	11	1181da7726bc5181d26b4e599270e97b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/tuihuijianlist.html	8	18205f8630ee99620982e443b289abf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/wssbdeptlist.html	2	94c17e95bcaa430cded4241533c8b3c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/wssbpermlist.html	5	0c3d56f4fc7df0d9de11dea4627b6432
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/wssbregiondeptlist.html	2	94c17e95bcaa430cded4241533c8b3c7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/zaibanjian	8	8d21e60908d569fefca96a342b1cd2e4

list.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/wssb/zancunjianlist.html	8	1bad82201748c4b162280237c656ecfc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/zcy/╞≤╥┤├√│╞▒Θ╤».html	11	5a4fc42909b5514f0eaf3626cb77c626
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/zcy/╞≤╥┤╡╝╟.html	5	cceb5dd343c0859d28f26f0d71ff1502
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/zcy/╞≤╥┤╫ó▒ß.html	10	c147784645e7076be67144e3ae09b6d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/blue_website/zcy/╫╔╟┼▒Θ╔╪.html	7	78af124d448943078d9226bdffb41030
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/alone/┤Ñ╥│.html	4	a1eae4664683512818bb650a45e404bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/═╝┐┌└┤─┐.html	7	8c19b1baf6f6db5dc81539f7ba6c95f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/═╝┐┌└┤─┐_╬╙└┤─┐.html	3	23b62604157b2a2760196d25fd9919f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╨╙╞┤└┤─┐.html	8	d00f25a94fa3e94b056c5fca105660f1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╨╙╞┤└┤─┐_╬╙└┤─┐.html	3	024677fb36a3bb91a0ba35230e57ba17
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╧┬╪└┤─┐.html	9	fbf22a4a568b59a5fecd3af808c946f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╧┬╪└┤─┐_╢■╝╢.html	5	e151308e16ca8602c443f9896f9892c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╨┌╬├└┤─┐.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╨┌╬├└┤─┐_╕┐╝╢.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╨┌╬├└┤─┐_╬╙└┤─┐.html	4	1af4459bb6e40768970e70313e300570
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╫≈╞╖└┤─┐.html	4	ab774f9e9b2ce64a0f04b7eba150da84
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/╫≈╞╖└┤─┐_╬╙└┤─┐.html	4	74ebd09e7cad4bbe4276301715f4d2c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/channel/▒·╞╖└┤─┐.html	5	a4a90d2533009da81954188aeaf6572f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/comment/╞└┬╟▄└φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/comment/╬╥┤─╞└┬╙▒φ.html	5	5b7a08226b819acaa7deada6c9c23d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	bfd9d532a970b6118bdbe745432ce4

INF/t/cms/www/red/comment/▒Θ┐┤├└┬┴╣╪╕┤.html		04
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/common/│╒╣ª╠ß╧╨╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/common/┤φ╬≤╠ß╧╨╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/common/╥│├µ├╕╙╨╒╫╣.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/common/╨┴╧ó╠ß╧╨╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/═╝┐┌─┌╙▌.html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/╨╙╡─┌╙▌.html	8	791566c038b15593bb1d6ebe69eb4e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/╧┬╚╪─┌╙▌.html	9	7af83f7dab3e0d0e6723d456477199e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/╥┐┴┤─┌╙▌.html	8	e26ca70d40d6cad2b72203c3f5251477
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/╫≈├╥─┌╙▌.html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/▒·├╥─┌╙▌.html	8	6fb43f02d4406dcc831c93229c51d529
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/inc_comment_input.html	3	6cdd7ccfd9980fca3d628b7f26a342d3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/content/inc_comment_list.html	1	5ebf5dcd0403038a06f1c2e8f614f1a0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/csi/╕ß└▒╟╓╝.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/csi/├└┬╙╨▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/csi/╣╓╕ µ.html	2	d274b8f792bdf33da6a05ef7e2e85606
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/csi/╣╓╕ µ▒µ╬╓.html	3	2840bddf26d837d73bb9f3932394e152
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/guestbook/┴⌠╤╙Ω╘┐.html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/guestbook/╬╥┤└┴⌠╤└╙▒φ.html	5	b4c8cab4ead68b5fe10f2193bcb30183
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/guestbook/▒Θ┐┤┴⌠╤╓╣╪╕┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/═╣├▒└┐.html	2	1aa8f3f08d07a4683a9fc3b06203f3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-	2	83a535bdab827d319497bee72f3d4b

INF/t/cms/www/red/include/╡╟┬╝.html		ca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/╥│═╖╡╝╟╜ └┐.html	2	cde19226de48cba19e1e42cdef5255bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/╥│═╖╡╟Ñ └┐.html	1	0c274a91ce902366856f3cec846ad92b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/╥│═╖╖┌┬╥≈ └┐.html	1	329bbc3e0e514299d5a87e1ccd50b312
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/╥│╜┼╙╤╟Θ┴┤╜╙ └┐.html	1	416d750f6bc37c48227ac5c673e30992
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/╥│╜┼╨┴ó └┐.html	2	3e1f48cc4c523aefc1893b8a2e0e8037
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/include/header_register.html	2	4cba08291225ba0ae8f690cb87601d79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/index/╨╟╥│.html	15	23918cbf24dd7b4a8559614f04a7f3c4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/═╟╕σ┴╨▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/═╟╕σ╨ ▌╕ ─╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/═╟╕σ╨Σ╚δ╥│.html	7	7615a9f9f0461d731e3e10b249938184
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/ ╒╥╕╪├▄┬δ╜ß╣ √╥│.html	4	8119a749811cd6788cfc33ab7df8e5f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/ ╒╥╕╪├▄┬δ╨Σ╚δ ╥│.html	5	41516152dbd244f5bcc6d1122efb9302
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒═╖╧±╨ ▌╕ ─╥│.html	4	7387641ee97790b8dbb38864747bd016
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒╔╨╨─╥│.html	4	b8d921c509280c0d46f21463668d4289
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒╔╨╨─╥│_╡ ╝╟╝.html	2	20ff410815c5c193cd0bfb629010eeef
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒╔╨╨─╥│_╥ │═╖.html	1	f115c1095e7941e7f42107bc1cb8d649
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒╔╨╨─╥│_╥ │╜┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒╔╨╨─╥│_╥ │╢Ñ.html	1	1ac6606ba30bf4065e940fb9f58a01bf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╕ß └▒├▄┬δ╨ ▌╕ ─╥│.html	3	b731e1f96d6f2188035b0795fbf19240

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╖ß└▒ ╟┬╜╥│.html	7	0781c15bc9a1b7f435431308802eb7ee
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╖ß└▒╨┤≐ó╨ ╠─╥│.html	6	2e6943e66e60047574f5db891f3d373a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╖ß└▒╬ó▓ß╥│.html	8	60e47bc3591623248c373969f4760f84
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╜ñ╖ε│ ╒╣ª╥│.html	4	5be027c684e03b03bce0adc38d3ad300
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/ ├▄┬δ╓╪╥├┬│.html	4	eb2a01069b666f590f6f7ee2153e5f6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/ㅔ ╟┬╜╫┤ ╠¼╥│.html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╧ ┌▓╪└╙▒φ╥│.html	5	a00123423e284e96db5d8aea5954deeb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/╫ó▓ß╜ß╣√╥│.html	4	e7d12b726b0e1cb6d7cb65b3e0b8a31f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/ ╒─┌└┤╣■└φ╥│.html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╕╪╡┤╥│.html	4	4a99ed086e3e9b7ade428de35265c225
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╖ó╜ ■≐Σ.html	4	8e1b3bdb8c33f3a196f90b008accf3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╖ó╨└╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/ └¼╖ °≐Σ.html	4	4cc580ef4385f28cd6957a10e871d028
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╨╒ ■≐Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╨└≐ó└─╟┴╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/╨╠ ─╨└≐ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/message/▓ ╕ σ╧Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/═╢ ╞▒╨ß╣√╥ | .html	5	d982ee772b37dcc69ce0163a764aea87
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/═╢ ╞▒╟ß╨╕╥ | .html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/═╢ ╞▒╧Σ└δ╥ | .html	1	3df0cbfd78067fc65548fd492b13385b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/ ╞└┬╥ | .html	5	be843242d7a1d606576de28d1892cc28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/╤╤╥≈╨ß╣√╥ | .html	4	decc1f8c3d4519857d65d3263169f48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/╤╤╥≈╧Σ└δ╥ | .html	4	b9c6784384d78a7d45cd653c152125f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/┴⌠╤╞▒σ└α▒≡╥ | .html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/┴⌠╤╞▒σ╧╠╥ | .html	12	033f978b50f64e84ab229ca0c96a9b73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/┴⌠╤╞▒σ╧Ω╟Θ╥ | .html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/▒Ω╟⌐┤╝ ╢╨╥ | .html	3	fdeaa32873e1a172e6ef73ca22a92913
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/▒Ω╟⌐╧Ω╟Θ╥ | .html	4	3f905c5ddea0680e6c36d40ba72ef786
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/style_page/content.html	1	0083887e27c572e0b7a4d553978d330e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/topic/╫¿ ╟Γ─¼ ╚╧╥ | .html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/red/topic/╫¿ ╟Γ╡╝ ╢╨╥ | .html	3	327dfb80de1d22dba5b06dc47ae7b6f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/alone/╡ Ñ╥ | .html	2	ca719ac9fb6517b48b05b20bed674fe9
/WebHallCMSV3.0BAProject/WebRoot/WEB-	3	5002a68f712e827e89c945d8790981

INF/t/cms/www/yellow_hr/channel/╩┬ ╘╪└┤─ ┐_╣■╝╣.html		50
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/channel/╨┬╪┼ └┤─ ┐_╨┬╪┼┴╨▒φ╥│.html	2	d19e0380e64465f92f958ebcfbd2fbf9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/comment/╞└┬▐╣■ └φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/comment/╬╥┤─╞└ ┬▐┴╨▒φ.html	5	5b7a08226b819acaa7deada6c9c23d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/comment/▒Θ┐┤╞└ ┬▐╕╪┐┤.html	2	bfd9d532a970b6118bdbe745432ce404
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/common/│╔╣ª╠ß╩ ╡╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/common/┤φ╬≤╠ß ╩╣╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/common/╥│├µ├╕╚ ╩┌╥╣╝.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/common/╨┴╩ó╠ß╩ ╡╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/content/╩┬ ╘╪─┌╚ ▌.html	5	e48717cd824eebf649f8f9c158944739
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/content/╨┬╪┼──┌╚ ▌_╨┬╪┼╝≥┤Ñ─┌╙▌╥│.html	3	2c1ade405a11d85a1c579f9ff05d2c75
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/content/╨┬╪┼──┌╚ ▌_╨┬╪┼╩Ω╧┐─┌╙▌╥│.html	4	c4f79dcc0558b846f6df2484d84ddb59
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi/╕ß└▒┤ ╟┬╝.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi/╞└▐┴╨▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi/╣┐┐µ.html	2	a9f92b7f8f5b888691632aafa2ad6e2a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi/╣┐┐µ▒µ╬╗.html	3	ea07949812230fad9bc69eb92310d06c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi_custom/┴¬╡┤╬ ╥├╠.html	3	6b0b7fdced499cfac8a796cf25cf0c8c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/guestbook/┴⌠╤╧ Ω╧┤.html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-	5	b4c8cab4ead68b5fe10f2193bcb3018

INF/t/cms/www/yellow_hr/guestbook/╬╥┤╼┻⌠╤┣┻╨▒φ.html		3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/guestbook/▓Θ┐┤┻⌠╤╘╪┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/═╢╥▀┻╨▒φ╥│.html	5	f8cadf1bc54088246a248e98b505471c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/═╢╥▀╨Σ╚δ╥│.html	9	952c7477ab7303945ec1329a7d908931
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/═╢╥▀▓Θ┐┤╥│.html	4	062e702a23410c9792cc9a42671b8499
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/╗Ñ╢»╝╗┻≈.html	2	360d8dc1e17a390445a798d04a639ceb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/ └┌╧▀╖ ├╠╕ ┴╨ ▒φ╥│.html	5	49c4f245af075c6d68c1f951452a7da8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/ ├±╥Γ ┌≈╝»═│╝ ╞┣╨▒φ.html	6	de766538b92e9223673f2c501f373722
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/╫╒╤»┴╨▒φ╥│.html	5	6458ce45baf51eb3424f7d2b93286896
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/╫╒╤»╨Σ╚δ╥│.html	7	29d76bec82c13b220e808d332ed5776b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/hdjl/╫╒╤»▓Θ┐┤╥│.html	4	46777930272ee8a8cd76fe79a9107ab4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/┤▀▓∩┤╫┗╤▓╪┌╨╞╣.html	1	184f3053da7edc52d71253c548322ae0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╗Ñ╢»╞╝╟¿.html	2	d2684da3492d8e1bdf034ce00dee33c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/┗╤▓╪┌▪▓▀.html	1	c411c63f35671930827e03a43e56b107
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/┗╤▓╪╖┬▓╒.html	1	cc846ae17255258739772ff322494461
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/┗╤▓╪╟╪°.html	1	919b38e9d174f11ef2be0a9d4ac08677
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╟°╚≥╝Θ╒▀.html	1	b50f60c802577d70a779ab6750ec3620
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╦√╒╝ ╓«╩» .html	1	89859fabdbd9fde763c51f26f0dd04a7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╧┬ ╘╪¿╟°.html	1	ed759eac57ccb2b6eb54af97b235ed63

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╨┬╬┼╢»╠¼.html	1	b3fd68f2ee7d24284019e14f7d356fa9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/┴∞┤╝╝▓╖▒.html	1	0bcebdfb06bef55514314b3588b5972d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/╨ú╞≤╟╧╬≈.html	1	ef685c4b78c71c72a43b673ce8f74923
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/bottom.html	1	b5a0b3b3c1bfede05482b5246b7b6a06
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/left.html	2	121a004c9f618201636950d192a37e26
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/left_hr.html	2	8a6c1120305f60f4a4a906458e1b9dfb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/include/top.html	7	142cb3fd00a56ceef56bcc155722c59c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/index/╨╬╥│.html	7	eb183607f7804253fc8702ccc4a5d76c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╝°╢╙▓Θ╤»╨┼╧ó.html	4	9614509cf1ae7132c25af3206098d4a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╥┤╬±╧Ω╧╕╨┼╧ó.html	3	10273accc468d2bdea93dcd57593bfaa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╨┬╧ε╖╥└α┴╨▒φ.html	6	68f9003bbe86c139baaae5f50a4dcf28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╨┬╧ε┴╨▒φ.html	7	6d8027b25d1d211172dfaebaf1111873
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╨┬╧ε┴╨▒φ_╨╒├√.html	6	448e3a8879fb4d2d0d9c19b8dbe0119b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╨┬╧ε╧Ω╧╕╨┼╧ó.html	12	536fe7441a29510fbdd2256f36c85a1f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╨┬╧ε▒φ┐±╧┬╘╪.html	5	ab1e821a3d831cd23271a00d335e0773
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/╫╔┬»═╢╦■╨┼╧ó.html	6	26957be4c882aac7d1cb53fc65a89e4e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/lawguide/▓┐ ├┼┴╨▒φ.html	3	01f07a2cea607f674c4b4aeef360dbb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╕ σ┴╨▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╕ σ╨ ▌╕ ¬╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╕ σ╨Σ╚	7	76159a9f9f0461d731e3e10b249938184

δ╥│.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╦▀└┴▒φ╥│.html	6	71a41adcc656dabd9e9fb97e2e0234cb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╦▀┴▌╤─╥│.html	8	6d4b3aceaa936e79aa31d4a1ad746f7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╦▀┴Σ└δ╥│.html	8	ccbd1ceb4e6140c2b6699652e6609e6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═╢╦▀▓Θ┐┤╥│.html	4	6da24927bf3ae5e484874028ba36aee1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═°╒╪╡≈▓Θ╩ß╣√╥│.html	4	cb6f31e869df020497d74c9630fb0985
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═°╒╪╡≈▓Θ┴┴▒φ╥│.html	6	b3f9c9c2c7da49e438bdf3d4a467080c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/═°╒╪╡≈▓Θ└└Σ└δ╥│.html	3	a45b7cdfcc23eb03ff366d2cd4004b86
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ╔╥╕╪├▄┬δ╩ß╣√╥│.html	2	3e0433d17d1577661c3bac269f6f7a9d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ╔╥╕╪├▄┬δ└└Σ└δ╥│.html	4	3e58f4c1df4189f38e3b8fa0922de548
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╡÷└╦╫┘┴┴▌─╥│.html	12	a6a2a0a43c618d52a78cd60bc332e1c9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒═╗╧±╩▌─╥│.html	4	7387641ee97790b8dbb38864747bd016
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒╔╩╩─╥│.html	4	7955355671e579e1303645aa9803ec23
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒╔╩╩─╥│_╡╝╣╢╣.html	3	8bade4ea04792ae1c32c144282946728
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒╔╩╩─╥│_╥│═╖.html	2	3272ec52a4c77136352a53e75bc4e832
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒╔╩╩─╥│_╥│╣┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒╔╩╩─╥│_╥│╢Ñ.html	1	83b2c77379ee566bb216a550b8a51df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒├▄┬δ╩▌─╥│.html	3	c91871d2541b79fdd86dfd020204f3e7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╖ß└▒┤╟┬╣╥│.html	4	23b3d7ba03250a2a17620569d77b78d0
/WebHallCMSV3.0BAProject/WebRoot/WEB-	12	21a5b137868b27a5e473730a4fb7fa9

INF/t/cms/www/yellow_hr/member/╕ß╘▒┴┴ó╨▐╤─╥|.html		7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╕ß╘╪ó▓ß╥|.html	11	a73aaec5d114d1b794762c6aee51ca45
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ╘ñ ╙┴╨▒φ╥|.html	5	5f7d77f90def431f4ca15ab643a9c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ╘ñ ╙╨Σ╚δ╥|.html	8	de8a6eacbaae5e3a1f51f7d37173689d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ╘ñ ╙╨Σ╚δ╥|2.html	7	6f3cade0051808d3c61673505f215ade
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╜°╣ ╙▓Θ╤»╨┴┴ó_╕ß╘▒╓╨╨.html	4	8c7362e59c20be821c77966da0861074
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╜ñ╕ε|╒╣ª╥|.html	4	54eac56df0f10bf9d39b95cb3d61aab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/ ├▄┬δ╓╪╥├╥|.html	3	4b4bad0cbc3237129faf752d55430e4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/┤ ╟┬╜╪┤ ╠¼╥|.html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╥Γ╝√╨Σ╚δ╥|.html	7	f1416b8bb5f7370d7eaa262cfa713eb7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╨╒╪┴┴▒φ╥|.html	5	a00123423e284e96db5d8aea5954deeb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╪╔╥»┴┴▒φ╥|.html	6	b6fcb7da50a6776d33df64cc55b85ede
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╪╔╥»╨▐╤─╥|.html	7	296c0016c8770b02e78317b5c69ef4e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╪╔╥»╨Σ╚δ╥|.html	7	1c3bcbc46fa6bb3e82b0ef36edb6e773
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╪╔╥»▒Θ┐┤╥|.html	3	38a754edbef20666d43a7a7226c98129
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/╪ó▓β╨ß╣√╥|.html	3	3f2d8b95b8c186811d5fc36bf09337cb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/ ╒═┌╨┼ ╣▄└φ╥│.html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╖╪╕┤╥│.html	4	4a99ed086e3e9b7ade428de35265c225
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╖ó╝▪╧Σ.html	4	8e1b3bdb8c33f3a196f90b008accf3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╖ó╨┼╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/ └¼╖°╧Σ.html	4	4cc580ef4385f28cd6957a10e871d028
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╨ ╒╝▪╧Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╨┼╧ó ╘═╢ ┴╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/╨ ▐╕ ─╨┼ ╧ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/message/▓ ╕ σ╧Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/opinionrecord/├±╥ Γ ╒≈╝»_╧Ω╧╕ .html	3	55df13942005e72ed5537133b0627e31
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/opinionrecord/├±╥ Γ ╒≈╝»═│╝ ╞.html	5	5feec28528d68d2959bda47b3241de7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/opinionrecord/├±╥ Γ ╒≈╝»┴╨▒φ_╕ ÷ ╚╦.html	5	8b363585c63e65db0bc1d642d3d12fb1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/opinionrecord/╥Γ╝ √╨Σ╚δ╥│.html	7	91f9b496344257642e9f16b7ef2d9b7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/═╢ ╞▒╝ ß╢√ ╥│.html	4	3c1cce8af2d72bf67d839b56448eda83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/═╢ ╞▒╟ß╝╕ ╥│.html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/═╢ ╞▒┴╨▒φ ╥│.html	6	b8f2178caf3970d9dae32a141fd61acd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/═╢ ╞▒╨Σ╚δ ╥│.html	3	3476d2c65d1ec85809be9099d82c5069
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/╞└┬╥│.ht	5	be843242d7a1d606576de28d1892cc28

ml		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/╥┬┬╥≈╜ß╣√╥|.html	4	decc1f8c3d4519857d65d3263169f48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/╥┬┬╥≈╜ß╣√╥|2.html	3	97436e236fa9ff1d23b1c3c16489e251
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/╥┬┬╥≈╨Σ╚δ╥|.html	4	b9c6784384d78a7d45cd653c152125f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/┴⌠╤└▒σ└α▒≡╥|.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/┴⌠╤└▒σ╨╫╥|.html	12	033f978b50f64e84ab229ca0c96a9b73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/┴⌠╤└▒σ╧Ω╟Θ╥|.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/▒Ω╟⌐┤╝╟╜╥|.html	3	fdeaa32873e1a172e6ef73ca22a92913
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/▒Ω╟⌐╧Ω╟Θ╥|.html	4	3f905c5ddea0680e6c36d40ba72ef786
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/style_page/content.html	1	0083887e27c572e0b7a4d553978d330e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/topic/╫┐╠Γ─¼╙╙╥|.html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/topic/╫┐╠Γ┤╝╟╜╥|.html	3	327dfb80de1d22dba5b06dc47ae7b6f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_hr/webmap/═° ╒┤╪═══╝╨╨▒Φ╥|.html	3	04bdf9cc4e3d99a56a57a9aee42f9166
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/alone/┤Ñ╥|.	2	1c9e089bc80459f0b67c8f0e58d90378

html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/═╝┐┌└┬┐.html	7	8c19b1baf6f6db5dc81539f7ba6c95f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/═╝┐┌└┬┐_╫╙└┬┐.html	3	23b62604157b2a2760196d25fd9919f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨╙╞┤└┬┐.html	8	d00f25a94fa3e94b056c5fca105660f1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨╙╞┤└┬┐_╫╙└┬┐.html	3	024677fb36a3bb91a0ba35230e57ba17
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╧┬╘╪└┬┐.html	9	fbf22a4a568b59a5fecd3af808c946f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╧┬╘╪└┬┐_╢■╝╢.html	5	e151308e16ca8602c443f9896f9892c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_| úµ √╬╨╠Γ.html	2	2f7a67fecde5855a85bfad31b322b0d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_╕╖╝╢.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_╕╖╝╢2.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_╛ i╙¬─╔▒.html	7	232afbdd3d329bd8bb989cee8506f9f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_╫╙└┬┐.html	4	1af4459bb6e40768970e70313e300570
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐_╫╙└┬┐2.html	2	baeecf7209fd06cad1c9a9f0698d5eb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╨┬╬┼└┬┐2.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╬≈╞╖└┬┐.html	4	ab774f9e9b2ce64a0f04b7eba150da84
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/╬≈╞╖└┬┐_╫╙└┬┐.html	4	74ebd09e7cad4bbe4276301715f4d2c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/channel/▒·╞╖└┬┐.html	5	a4a90d2533009da81954188aeaf6572f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/comment/╞└┬╟▄└φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-	5	5b7a08226b819acaa7deada6c9c23d

INF/t/cms/www/yellow_research/comment/╬ ╥ᅻ─╞ᄂ▉ᄇᄈ▒φ.html		5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/comment/▓ Θ게╞ᄂ▉╗╪ᅦ.html	2	bfd9d532a970b6118bdbe745432ce404
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/common/│╔ ╣ª╟ß╨╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/common/┤φ ╬≤╟ß╨╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/common/╥│ ├µ├╕ ╙╙ ╒╥ᅻ╜.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/common/╨┼ ╧ó╟ß╨╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/═╝┐ ┌─┌▉ .html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╨╙╞ ᅻ─┌▉ .html	8	791566c038b15593bb1d6ebe69eb4e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╧┬ᄂ ╪─┌▉ .html	9	7af83f7dab3e0d0e6723d456477199e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╨┬╬ ┼─┌▉ .html	8	e26ca70d40d6cad2b72203c3f5251477
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╨┬╬ ┼─┌▉ _│ú╝ √╬╨╟Γ.html	5	969bc3500f49ef95a033f733669b5c8b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╨┬╬ ┼─┌▉ 2.html	5	aecb0a3a50ab6552af010df9d1d1844d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/╬≈╞ ╥─┌▉ .html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/▓·╞ ╥─┌▉ .html	8	6fb43f02d4406dcc831c93229c51d529
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/inc_comment_input.html	3	6cdd7ccfd9980fca3d628b7f26a342d3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/content/inc_comment_list.html	1	5ebf5dcd0403038a06f1c2e8f614f1a0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/csi/╖ß ᄂ▒ᅻ ╠ ┬╝.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/csi/╞ᄂ▉ᄇᄈ ▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/csi/╣ㅁ╕ µ.html	2	a9f92b7f8f5b888691632aafa2ad6e2a

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/csi/╣╓╕µ▒µ╬╗.html	3	ea07949812230fad9bc69eb92310d06c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/guestbook/┴⌠╤╙Ω╧╕.html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/guestbook/╬╥┤—┴⌠╤╘┴▒φ.html	5	b4c8cab4ead68b5fe10f2193bcb30183
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/guestbook/▓Θ┐┤┴⌠╤╓╕╪┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/═╢╦▀┴╨▒φ╥│.html	5	f8cadf1bc54088246a248e98b505471c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/═╢╦▀╨Σ╚δ╥│.html	9	952c7477ab7303945ec1329a7d908931
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/═╢╦▀▓Θ┐┤╥│.html	4	062e702a23410c9792cc9a42671b8499
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/╕Ñ╢»╝╕┴≈.html	2	360d8dc1e17a390445a798d04a639ceb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/├±╥┌╒≈╝»═│╝╞┴▒φ.html	5	d0ae5c5cda2bb935727a2a35ecaff043
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/╬╓╤»┴╨▒φ╥│.html	5	8e19d8568c8ab01b13a17fedf64acbf9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/╬╓╤»╚Σ╚δ╥│.html	7	32369b53104a94dc3fed3e9de0e708d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/hdjl/╬╓╤»▓Θ┐┤╥│.html	4	e61a5f7ac30f35e45cdb15b4c45a5bd7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/═╢╞▒└╕.html	2	df2dcf97c712a39be416b301b085a0fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/┤╟┬╝.html	2	83a535bdab827d319497bee72f3d4bca
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/╥│═╕╣╝└╕.html	2	cde19226de48cba19e1e42cdef5255bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/╥│═╖Ñ└╕.html	1	0c274a91ce902366856f3cec846ad92b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/╥│═╖╒┌≈└╕.html	1	329bbc3e0e514299d5a87e1ccd50b312
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/╥│╝	1	416d750f6bc37c48227ac5c673e30992

┼╨╤╟Θ└┤╩╨└╕.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/╥│╩┼╨┼╧ó└╕.html	2	3e1f48cc4c523aefc1893b8a2e0e8037
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/▒∞╩■.html	4	9b989fa97733ef17cb0598c8e8b652e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/bottom.html	1	75858533fe7cc5aec04501db7f24fe43
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/header_register.html	2	4cba08291225ba0ae8f690cb87601d79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/include/top.html	4	fe8e2df59885b89c6b6a30e0ac44eb1b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/index/╩╬╥│.html	12	6913563f17e22229b770e8b6ff7d9964
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩∘╣▓Θ╤»╩┼╧ó.html	4	9614509cf1ae7132c25af3206098d4a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╥╡╬±╧Ω╧╕╩┼╧ó.html	3	d4230f3a03edbd586266bc53ce6c6c92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩┬╧ε╥╓└α└╩▒φ.html	6	5a4d270daaef2d88d17b149c0e4ac1e4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩┬╧ε└╩▒φ.html	7	c7d142dc2c402163f8f00f38e032ee80
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩┬╧ε└╩▒φ_╩╒├√.html	6	6ce239aa85ecede6dbf49e4926f744f9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩┬╧ε╧Ω╧╕╩┼╧ó.html	6	56f61869e205d89fbc8694c5043ffb6f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╩┬╧ε▒φ╕ ±╧┬ ╞╪.html	5	ab1e821a3d831cd23271a00d335e0773
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/╫╔╤»═╢╗■╩┼╧ó.html	6	26957be4c882aac7d1cb53fc65a89e4e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/lawguide/▓╕├┼└╩▒φ.html	3	01f07a2cea607f674c4b4aeef360dbb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╕σ└╩▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╕σ╨ ▌╕ ─╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╕σ╨Σ╚δ╥│.html	7	7615a9f9f0461d731e3e10b249938184
/WebHallCMSV3.0BAProject/WebRoot/WEB-	6	71a41adcc656dabd9e9fb97e2e0234c

INF/t/cms/www/yellow_research/member/═╢╒▀┴╨▒φ╥│.html		b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╒▀╨▐╕─╥│.html	8	6d4b3aceaa936e79aa31d4a1ad746f7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╒▀╨Σ╚δ╥│.html	8	ccbd1ceb4e6140c2b6699652e6609e6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═╢╒▀▒Θ┐┤╥│.html	4	6da24927bf3ae5e484874028ba36aee1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═°╒╪≈▒Θ╝ß╣√╥│.html	4	cb6f31e869df020497d74c9630fb0985
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═°╒╪≈▒Θ┴╨▒φ╥│.html	6	a5c0b19fc50d152fa5f04f8d6c88ec33
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/═°╒╪≈▒Θ╨Σ╚δ╥│.html	3	a45b7cdfcc23eb03ff366d2cd4004b86
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ ╒╥╕╪├▄┬δ╝ß╣√╥│.html	3	58a087e00e7331974b25ffa2d3bb8d0e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ ╒╥╕╪├▄┬δ╨Σ╚δ╥│.html	5	fd95541d37dbc2d8f1fdc2fcb60fa48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└═╖╧±╨▐╕─╥│.html	4	7387641ee97790b8dbb38864747bd016
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╒╨╨─╥│.html	4	7955355671e579e1303645aa9803ec23
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╒╨╨─╥│_╡╣╝╢.html	3	8bb43e457d51467b320bd7aa6a572856
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╒╨╨─╥│_╥│═╖.html	2	3272ec52a4c77136352a53e75bc4e832
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╒╨╨─╥│_╥│╝┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╒╨╨─╥│_╥│╢Ñ.html	1	83b2c77379ee566bb216a550b8a51df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└├▄┬δ╨▐╕─╥│.html	3	08e3b061ddcaa727912e2ed0fe1ae596
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╡╟╥╝╥│.html	4	a7f44bcf528e4bad75becc191809089f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╨┼╧ó╨▐╕─╥│.html	13	8ff8ed0391b28649c326fd923e928f29
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╕ß└╬ó▓ß╥│.html	16	02669ccc72b5652aa31995a57a52fa06

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㄣñ ㅂㅗㅛ▒φ╥|.html	5	5f7d77f90def431f4ca15ab643a9c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㄣñ ㅂㅛΣㄴδ╥|.html	8	de8a6eacbaae5e3a1f51f7d37173689d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㄣñ ㅂㅛΣㄴδ╥|2.html	7	6f3cade0051808d3c61673505f215ade
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㅛ∘ ╢ㄴ▓Θ╤»ㅛㅏㅗó_╕ß ㄴ▒╓ㅛㅡ.html	4	8c7362e59c20be821c77966da0861074
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㅛñ ╕ε|╒╢ª╥|.html	4	54eac56df0f10bf9d39b95cb3d61aab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/├■ ┬δ╓╪╓├╥|.html	3	4b4bad0cbc3237129faf752d55430e4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㅓ╟ ┬ㅛ╫┤ ╟¼╥|.html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/ㅛ╒ ▓╪ㅗㅛ▒φ╥|.html	5	a00123423e284e96db5d8aea5954deeb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╪╓ ╤»ㅗㅛ▒φ╥|.html	6	88a744027e218ba03bfd98de19454cc5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╪╓ ╤»ㅛ▐ㅟ─╥|.html	7	3d93b1f2cad3ef056cf379d53dce507d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╪╓ ╤»ㅛΣㄴδ╥|.html	6	f28df86bd55de06232595d6febd321ae
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╪╓ ╤»▓Θ┐┤╥|.html	3	9ffeb79431b2076525781da32a94a5a8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/╪ó ▒ß╝ß╣√╥|.html	3	f4efab974418f639d3ada36837d07bc4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╒ ─┌╨┤╣▄└φ╥|.html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╕╪	4	4a99ed086e3e9b7ade428de35265c225

╕┤╥│.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╖ó╝▄╧Σ.html	4	8e1b3bdb8c33f3a196f90b008accf3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╖ó╨┼╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/└¼╕°╧Σ.html	4	4cc580ef4385f28cd6957a10e871d028
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╧╒╝▄╧Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╨┼╧ó└─╢┴╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/╨▌╕─╨┼╧ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/message/▓╕σ╧Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/opinionrecord/├±╥Γ╒≈╝»_╧Ω╤╕.html	3	ae40da04feec231a37fe2f2194790110
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/opinionrecord/├±╥Γ╒≈╝»═│╝╞.html	5	5feec28528d68d2959bda47b3241de7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/opinionrecord/├±╥Γ╒≈╝»┴╨▒φ_╕÷╚╦╥.html	5	f8860310842097768135 6af1716de74b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/═╢╞▒╝ß╡√╥│.html	4	3c1cce8af2d72bf67d839b56448eda83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/═╢╞▒╞ß╨╗╥│.html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/═╢╞▒┴╨▒φ╥│.html	6	b8f2178caf3970d9dae32a141fd61acd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/═╢╞▒╧Σ╚δ╥│.html	3	3476d2c65d1ec85809be9099d82c5069
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/╖╥└α▓Θ╤»┴╨▒φ╥│.html	2	e5797f2d216b47f23396f75055a31dfd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/╚╤╟Θ└┤╝╚┌┌┌≈╝ß╡√╥│.html	2	b953a01e99a66cd652bcd05e0a8007fc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/╞└┬▀╥│.html	5	be843242d7a1d606576de28d1892cc28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/╥┌┌┌≈╝ß╡√╥│.html	4	decc1f8c3d4519857d65d3263169f48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-	3	97436e236fa9ff1d23b1c3c16489e25

INF/t/cms/www/yellow_research/special/╦╦╦≈╜ß╣√╥|2.html		1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/╦╦╦≈╩Σ╚δ╥|.html	4	b9c6784384d78a7d45cd653c152125f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/┴⌠╤╘▒σ└α▒≡╥|.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/┴⌠╤╘▒σ╩╢╥|.html	12	033f978b50f64e84ab229ca0c96a9b73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/┴⌠╤╘▒σ≒Ω╟Θ╥|.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/▒Ω╟⌐┤╜╢╜╥|.html	3	fdeaa32873e1a172e6ef73ca22a92913
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/▒Ω╟⌐≒Ω╟Θ╥|.html	4	3f905c5ddea0680e6c36d40ba72ef786
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/style_page/content.html	1	0083887e27c572e0b7a4d553978d330e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tool/╘┌═▀╢ñ╛▀└╩▒φ╥|.html	7	fbfea525baef3607543cbb3d62b5c53f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/tool/╜╞╦⌠╞≈.html	6	5b61ae37536a6cb9c59ff6334338234b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/topic/╬¿╠Γ─¼╙╥|.html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/topic/╬¿╠Γ┤╜╟╜╥|.html	3	327dfb80de1d22dba5b06dc47ae7b6f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/webmap/═°╒┤╪═══└╩▒φ╥|.html	5	f4a09fccff2a0d0f47eee4f0b32dea85

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/banjiejianlist.html	13	b89bcc62315221fae76f06606703bcf1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/busiindexlist.html	2	a9578dbd7f290ac074f7340fc00cfdff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/businesscouncillist.html	5	9e34ad06ac8d0174dba451d67f00b2a5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/busizxfwlist.html	2	d8e8d8e3ba9de8b2a1596d690537ddcc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/matter.html	10	1cad56afe1d54af995fee94e0747ec25
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/matter_╨╙╒■.html	10	b8576d9b290b2fa7165ac494d1e26161
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/matterdetail.html	11	2fb4e1f83de3acfa11c133760625b8e8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/matteredit.html	11	e8bad7bb72ff1f7501899f64a7c5a0dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/matteredit_╨╙╒■.html	11	7bac3c5cc458bb2ca24b5400e0255579
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/tuihuijianlist.html	8	d3d2e759eb0f0ba7dbcda08d2ff8549f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssb_download.html	3	8a17279a0c1868c2cbe68a13421c0600
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssb_lawguide.html	5	3ccd790d43f8110519b1babe5562a088
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssb_permbysort.html	5	e4d8897ab76c5ef9dd8cda4f20fec08d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssb_permissionitemsort.html	5	3a28ed19a66824db96d175ef55be6061
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssbdeptlist.html	3	147b8430cb3686af7228809b27a50582
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/wssbpermlist.html	6	885776a07f8b74565c6315f6324024b2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/zaibanjianlist.html	8	cca77b4d32f1227fa5cdf75df9cdb3fc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/wssb/zancunjianlist.html	8	a1cd862b7714058848a46f17591c77d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/zcy/╞≤╦┤├	11	5a4fc42909b5514f0eaf3626cb77c626

√| ├▒Θ╤».html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/zcy/ ╞≤╥┤┤ ╟╝ ╟.html	5	cceb5dd343c0859d28f26f0d71ff1502
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/zcy/ ╞≤╥┤╟ó ▒ß.html	10	c147784645e7076be67144e3ae09b6d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_research/zcy/╫╥╢┼▒Θ ╓╪.html	9	aa3ff3a05ea1388f2fcf0ec0d89d39ec
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/alone/┤Ñ╥| .html	4	a1eae4664683512818bb650a45e404bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/═╝┐Γ └┤─┐ .html	7	8c19b1baf6f6db5dc81539f7ba6c95f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/═╝┐Γ └┤─┐_╟╙└┤─┐ .html	3	23b62604157b2a2760196d25fd9919f2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨╙╞ ┤ └┤─┐ .html	8	d00f25a94fa3e94b056c5fca105660f1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨╙╞ ┤ └┤─┐_╟╙└┤─┐ .html	3	024677fb36a3bb91a0ba35230e57ba17
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╧┬└ ╪└┤─┐ .html	9	fbf22a4a568b59a5fecd3af808c946f5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╧┬└ ╪└┤─┐_╢■╝╢.html	5	e151308e16ca8602c443f9896f9892c6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐ .html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_| ú╝ √╬╧╠Γ.html	2	2f7a67fecde5855a85bfad31b322b0d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_╕╕╝╢.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_╕╕╝╢2.html	5	c5fa2f91b4e63b8bed85d69b5101d0fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_╡ ¡╙¬─╔╔▒.html	7	232afbdd3d329bd8bb989cee8506f9f6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_╟╙└┤─┐ .html	4	1af4459bb6e40768970e70313e300570
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐_╟╙└┤─┐ 2.html	2	baeecf7209fd06cad1c9a9f0698d5eb3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╨┌╬ ┼└┤─┐ 2.html	12	2c3a2a4bece5488832c2c003905c3a3d
/WebHallCMSV3.0BAProject/WebRoot/WEB-	4	ab774f9e9b2ce64a0f04b7eba150da8

INF/t/cms/www/yellow_webhall/channel/╬≈╞╥└┤─┐.html		4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/╬≈╞╥└┤─┐_╬╨└┤─┐.html	4	74ebd09e7cad4bbe4276301715f4d2c3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/channel/▒·╞╥└┤─┐.html	5	a4a90d2533009da81954188aeaf6572f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/comment/╞└┬╟▄└φ.html	7	c820881a3c0cd63168ac78a54ec2ec47
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/comment/╬╥┤─╞└┬▀└▒φ.html	5	5b7a08226b819acaa7deada6c9c23d5e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/comment/▒Θ┐┤╞└┬▀╕╪┤.html	2	bfd9d532a970b6118bdbe745432ce404
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/common/│╔╣ª╠ß╨╥│├µ.html	1	afe52cf639e12a032d52f10904abbb4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/common/┤φ╬≤╠ß╨╥│├µ.html	1	a0e7971f4575c8d19e8c417be05060f3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/common/╥│├µ├╕╙╨╒╥┤╜.html	1	8d6dbdfa82e8c0b896af69d1e27eab99
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/common/╨┴╧ó╠ß╨╥│├µ.html	1	c02f4238186536a9e00a5ee1d49da213
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/═╝┐Γ─┌▐ .html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╨╨╞┤─┌▐ .html	8	791566c038b15593bb1d6ebe69eb4e41
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╧┬└╪─┌▐ .html	9	7af83f7dab3e0d0e6723d456477199e3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╨┬╬┼─┌▐ .html	8	e26ca70d40d6cad2b72203c3f5251477
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╨┬╬┼─┌▐ _│ú╝√╣╨╠Γ.html	5	969bc3500f49ef95a033f733669b5c8b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╨┬╬┼─┌▐ 2.html	5	aecb0a3a50ab6552af010df9d1d1844d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/╬≈╞╥─┌▐ .html	12	6d141a7d622a2ad3a5fd0b078851edf4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/▒·╞╥─┌▐ .html	8	6fb43f02d4406dcc831c93229c51d529
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/inc_comment_input.html	3	6cdd7ccfd9980fca3d628b7f26a342d3

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/content/inc_comment_list.html	1	5ebf5dcd0403038a06f1c2e8f614f1a0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/csi/╕ß╘╡ ╟╥╝.html	1	b34e8763207bfdd6bdcfd856eafecdd6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/csi/ ╞╘┐▀╙╨▒φ.html	1	a3904741749cbc281de36e5773b25488
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/csi/╣⌐╕ µ.html	2	a9f92b7f8f5b888691632aafa2ad6e2a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/csi/╣⌐╕ µ▒µ╬╗.html	3	ea07949812230fad9bc69eb92310d06c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/csi_custom/my_custom.html	1	ecbcaac5d65ecfeca116d22ee67679f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/guestbook/┴⌠╤╙Ω┴╡ .html	3	86a236cd1925c9eeee743cc8b4b7a9ad
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/guestbook/╬╥┤—┴⌠╤╘╨▒φ.html	5	b4c8cab4ead68b5fe10f2193bcb30183
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/guestbook/▓Θ┐┤┴⌠╤╘╡╪┤.html	3	5f41474e81033e9a0b64ce6c4467eedc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/═╢╤▀┴╨▒φ╥│.html	5	f8cadf1bc54088246a248e98b505471c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/═╢╤▀╨Σ╚δ╥│.html	9	952c7477ab7303945ec1329a7d908931
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/═╢╤▀▓Θ┐┤╥│.html	4	062e702a23410c9792cc9a42671b8499
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/╕Ñ╢»╜╕┴≈.html	2	0f8c4d56d341c0a88112e1f818749a09
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/├±╥┌╒≈╜»═│╜ ╞┴╨▒φ.html	5	d0ae5c5cda2bb935727a2a35ecaff043
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/╪╔╤»┴╨▒φ╥│.html	5	8e19d8568c8ab01b13a17fedf64acbf9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/╪╔╤»╨Σ╚δ╥│.html	7	32369b53104a94dc3fed3e9de0e708d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/hdjl/╪╔╤»▓Θ┐┤╥│.html	4	e61a5f7ac30f35e45cdb15b4c45a5bd7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/═╢ ╞▒└╕.html	2	df2dcf97c712a39be416b301b085a0fe
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/┤ ╟╥╝	2	83a535bdab827d319497bee72f3d4bca

.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/╥│═╖╡╝╟╝└╕.html	2	cde19226de48cba19e1e42cdef5255bc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/╥│═╖╢Ñ└╕.html	1	0c274a91ce902366856f3cec846ad92b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/╥│═╖╒╒╒≈└╕.html	1	329bbc3e0e514299d5a87e1ccd50b312
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/╥│╝┼╙╤╟Θ╨┤╝╙└╕.html	1	416d750f6bc37c48227ac5c673e30992
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/╥│╝┼╙╨┼╧ó└╕.html	2	3e1f48cc4c523aefc1893b8a2e0e8037
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/░∞╝■.html	4	9b989fa97733ef17cb0598c8e8b652e9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/bottom.html	1	fcc971c686374e972241f1a2e5b4007a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/bottom2.html	1	8b2512726ed24d1b8a0fc6db91f30deb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/header_register.html	2	4cba08291225ba0ae8f690cb87601d79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/left.html	3	de2bd7ac5af70c13e3310656bdb0c41b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/left_fuwu.html	1	a865c6c555cdb8d2f83467b4ae3dee5b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/left_survey.html	1	c0bbe5b8a2b259bcbb9a315dc6feabf2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/top.html	6	02ee630cc0646b71710d10f687ca3668
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/include/top_login.html	5	5679587da62bbadfeee79e010032d13f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/index/╩╬╥│.html	26	e016e0a55a1a5aca85815b55b9d8951b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╝°╢╙▒Θ╤»╨┼╧ó.html	4	9614509cf1ae7132c25af3206098d4a3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╥┤╬±╧Ω╧┐╨┼╧ó.html	3	10273accc468d2bdea93dcd57593bfaa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╩┬╧ε╖╥└α┴╨▒φ.html	6	68f9003bbe86c139baaae5f50a4dcf28
/WebHallCMSV3.0BAProject/WebRoot/WEB-	7	6d8027b25d1d211172dfaebaf111187

INF/t/cms/www/yellow_webhall/lawguide/╨┬╧ε┴╨▒φ.html		3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╨┬╧ε┴╨▒φ_╨╒├√.html	6	448e3a8879fb4d2d0d9c19b8dbe0119b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╨┬╧ε╧Ω╤╕ ╨┼╧ó.html	12	2a0c7bf1ad9e2fbe52c04f18efc1f1b6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╨┬╧ε▒φ╕ ±╧┬ ╘╪.html	5	b0265d9ccd0246047bae0fd0ec63fd1e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/╫╔┬» ═╢╦▀╨┼╧ó.html	6	26957be4c882aac7d1cb53fc65a89e4e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/lawguide/▓┐ ├┼┴╨▒φ.html	3	29f5f1f79942a810130d384071ecef79
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╕ σ┴╨▒φ╥│.html	5	97f1ff252bb7a764b0bf9d14755be222
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╕ σ╨ ▌╕ ─╥│.html	7	25a0f9a714922f9c06bc402da1f2766e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╕ σ╨Σ╚δ╥│.html	7	7615a9f9f0461d731e3e10b249938184
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╓ ■┴╨▒φ╥│.html	6	9eaf3458763be093602b02b2d75ccfd9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╓ ■╨ ▌╕ ─╥│.html	8	6d4b3aceaa936e79aa31d4a1ad746f7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╓ ■╨Σ╚δ╥│.html	8	ccbd1ceb4e6140c2b6699652e6609e6d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═╢╓ ■▒Θ╕ ┤╥│.html	4	6da24927bf3ae5e484874028ba36aee1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═°╒ ╧┤ ≈▒Θ╨ ß╣√╥│.html	4	cb6f31e869df020497d74c9630fb0985
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═°╒ ╧┤ ≈▒Θ┴╨▒φ╥│.html	6	a5c0b19fc50d152fa5f04f8d6c88ec33
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/═°╒ ╧┤ ≈▒Θ╨Σ╚δ╥│.html	3	a45b7cdfcc23eb03ff366d2cd4004b86
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ ╒╥╖ ╪├▄┬δ╨ ß╣√╥│.html	3	58a087e00e7331974b25ffa2d3bb8d0e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ ╒╥╖ ╪├▄┬δ╨Σ╚δ╥│.html	5	fd95541d37dbc2d8f1fdc2fcb60fa48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╖ß╘ ▒═╖╧±╨ ▌╕ ─╥│.html	4	7387641ee97790b8dbb38864747bd016

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╔╓╨╨═╦│.html	4	7955355671e579e1303645aa9803ec23
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╔╓╨╨═╦│_┤╝╢╝.html	4	95aa11f84396c9d8756629f05724cad2
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╔╓╨╨═╦│_╦│═╗.html	2	3272ec52a4c77136352a53e75bc4e832
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╔╓╨╨═╦│_╦│╝┼.html	2	62e89e07e14e570c0fa509ad5468fb92
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╔╓╨╨═╦│_╦│╣Ñ.html	1	83b2c77379ee566bb216a550b8a51df1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒▐┬δ╨▐╣╤╦│.html	3	08e3b061ddcaa727912e2ed0fe1ae596
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒┤╟┬╝╦│.html	4	204ee724d7fef8648fab7a3fb0b29e52
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╨╪╧ó╨▐╣╤╦│.html	13	8ff8ed0391b28649c326fd923e928f29
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╗ß╘▒╪ó▓ß╦│.html	16	02669ccc72b5652aa31995a57a52fa06
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ └ñ╘▒╝─┌▌╦│.html	3	28f0c6ac53851054bc85384aa86650e4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ └ñ╘▒╝┴╨▒φ╦│.html	5	3c273193bbbfc2aa4ea0c44e0fbd586c
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ └ñ╘▒╝╨Σ└δ╦│.html	8	de8a6eacbaae5e3a1f51f7d37173689d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ └ñ╘▒╝╨Σ└δ╦│2.html	7	6f3cade0051808d3c61673505f215ade
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╝°╣└▓Θ╦»╨┤╧ó_╗ß╘▒╔╓╨═.html	4	76dfec9f811d822a3ed2c6f9b59d0ee6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╝ñ╗ε│╔╣ª╦│.html	4	54eac56df0f10bf9d39b95cb3d61aab9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/ ├▄┬δ╔╪╔├╦│.html	3	4b4bad0cbc3237129faf752d55430e4a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/┤ ╟┬ ╝╬┤ ╟¼╦│.html	1	0999ce85331296259f1d37db764a7e07
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/┤Ñ┤ ⌐┤ ╟┬╝╡ ▄╛ °╦│ ├µ.html	1	86cf8b55270eae9485b526ed0c44b6c5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╨╒▓	5	a00123423e284e96db5d8aea5954deeb

╪┴╨▒φ╥│.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╫╒»┴╨▒φ╥│.html	6	084530d7e0f1a2522347cd17dbe3875d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╫╒»╨▐╕─╥│.html	7	3d93b1f2cad3ef056cf379d53dce507d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╫╒»╨Σ╚δ╥│.html	6	d348de57ddcd0cd6a9e8dc1308af65ea
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╫╒»▓Θ┐┤╥│.html	3	9ffeb79431b2076525781da32a94a5a8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/╪ó▓ß╝ß╣√╥│.html	3	f4efab974418f639d3ada36837d07bc4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/iframe_upload.html	1	ca34b86701804c68be6bc28348e72ee5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/image_area_select.html	6	1e85461b665e64c32e513a8ad24539d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/image_cuted.html	1	f303c9b5299d22fd129bb49763a39c0b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/member/image_upload.html	3	d2660ff6cf99d2a69a22a2e3d578f965
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╒┘─┌╞▄└φ╥│.html	3	4b66ef80809f21e9202c51b11d118554
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╗╪╕┤╥│.html	4	4a99ed086e3e9b7ade428de35265c225
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╖ó╝▄╧Σ.html	4	8e1b3bdb8c33f3a196f90b008accf3f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╖ó╨┼╥│.html	4	330ed212dd6e329d5c6b1edb831230ac
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/└¼╗°╧Σ.html	4	4cc580ef4385f28cd6957a10e871d028
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╨╒▄╧Σ.html	4	44df6c95d8bb88636385e9cade3f99c1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╨┤╧ó╘─┴╥│.html	3	56cf0ea864fa34ee8955a8d938b4af73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/╨▐╕─╨┼╧ó╥│.html	3	8fd15fe342d2d52111804c59d66b196b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/message/▓╕σ╧Σ.html	4	8ef24adf70c6054c2e46b4d955a29c02
/WebHallCMSV3.0BAProject/WebRoot/WEB-	3	ae40da04feec231a37fe2f219479011

INF/t/cms/www/yellow_webhall/opinionrecord/├±╥┌ ┌≈╝»_╧Ω╤┤ .html		0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/opinionrecord/├±╥┌ ┌≈╝»═│╝ ╞.html	5	5feec28528d68d2959bda47b3241de7e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/opinionrecord/├±╥┌ ┌≈╝»┴╙▒φ_╕ ÷ ╚╥.html	5	f886031084209776813 56af1716de74b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/═╢ ╞▒╝ß╣√╥│.html	4	3c1cce8af2d72bf67d839b56448eda83
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/═╢ ╞▒╠ß╝╕╥│.html	4	53f7973007b92fbd7e7a0d8d6369f29b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/═╢ ╞▒┴╙▒φ╥│.html	6	b8f2178caf3970d9dae32a141fd61acd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/═╢ ╞▒╧Σ╚δ╥│.html	3	3476d2c65d1ec85809be9099d82c5069
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/ ╞└┐ ╥│.html	5	be843242d7a1d606576de28d1892cc28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/╥╥╥≈╝ß╣√╥│.html	4	decc1f8c3d4519857d65d3263169f48b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/╥╥╥≈╝ß╣√╥│2.html	3	3a741fd17fbc7e2234bb7d250a7e5672
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/╥╥╥≈╧Σ╚δ╥│.html	4	b9c6784384d78a7d45cd653c152125f0
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/┴⌠╤┣ ▒σ└α▒≡╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/┴⌠╤┣ ▒σ╧╟╥│.html	12	033f978b50f64e84ab229ca0c96a9b73
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/┴⌠╤┣ ▒σ╧Ω╟Θ╥│.html	1	c0d34657e3e157faf5ebbd02eba35a6b
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/▒Ω╟┌ ┤╝ ╢╝╥│.html	3	fdeaa32873e1a172e6ef73ca22a92913
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/▒Ω╟┌ ╧Ω╟Θ╥│.html	4	3f905c5ddea0680e6c36d40ba72ef786
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/special/RSS.html	1	220ff92a0939db2a5e96a01552e8e96e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/style_page/channel.html	1	27a942acfb993493d769c5b6d1f95507
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/style_page/content.html	1	0083887e27c572e0b7a4d553978d330e

/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/sync/╨²╛▌═¼▓╢╨┬ ╘÷┬│.html	3	a8276a6242204381996d1db55120d880
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/sync/╨²╛▌═¼▓╢╨└▒Φ┬│.html	6	aff734a64ab44ba1a0368b6dfce99947
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/sync/╨²╛▌═¼▓╢▒d╢ i┬│.html	3	a0c22cc8b94148c7dfca25c81e110fb9
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/tag/channel_list.html	1	d28336b412dd42e291877dabc1721f13
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/tag/channel_list_my.html	1	8c28879b13e6f68e81ef33c4faec9e7f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/tag/content_list.html	1	4aac40a07acb38616c642a998825c0d4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/tag/content_page.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/topic/╬┐╠Γ─¼╙┬│.html	11	6bd3b3a519181735f81814af5879e9fa
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/topic/╬┐╠Γ┤╣╟╨│.html	3	327dfb80de1d22dba5b06dc47ae7b6f4
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/banjiejianlist.html	14	e493c2ecbbadf31da0d61bd8b67b2239
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/busiindexlist.html	2	a9578dbd7f290ac074f7340fc00cfdff
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/businesscouncillist.html	5	9166185915cb177fe93184b995032ba6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/busizxfwlist.html	2	d8e8d8e3ba9de8b2a1596d690537ddcc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/matter.html	10	1cad56afe1d54af995fee94e0747ec25
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/matterdetail.html	11	2fb4e1f83de3acfa11c133760625b8e8
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/matteredit.html	11	e8bad7bb72ff1f7501899f64a7c5a0dd
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/tuihuijianlist.html	8	d3d2e759eb0f0ba7dbcda08d2ff8549f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssb_download.html	4	4463a78d1e660075a44278b3eb5c6b7d
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssb_la	11	7ef817a029b8362e5eaf1794d9a874af

wguide.html		
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssb_permbysort.html	6	1b9e86db2683a86b2f509d3e68ce7c6e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssb_permissionitemsort.html	5	c2c39e1fb09be0abf66769897758d4b7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssbdeptlist.html	3	d5205f52724ee53df9a800b011554ecf
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/wssbpermlist.html	6	2ffa4fc40f4a1d7204d5601d5abf21fb
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/zaibanjianlist.html	8	cca77b4d32f1227fa5cdf75df9cdb3fc
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/wssb/zancunjianlist.html	8	a1cd862b7714058848a46f17591c77d6
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/zcy/╞≤╥┤├√ | ╞▒Θ╤».html	5	ffcced7f0dbdc9161b72aff1673eb740
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/zcy/╞≤╥┤┤╟ ╝╟.html	5	5eb23400bb0d4b1e7ba5051bf7988084
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/zcy/╞≤╥┤╫ó ▒ß.html	4	f23fa456b30f2d99d2f66fd4c5e09f28
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms/www/yellow_webhall/zcy/╫╥╟┼▒Θ ╓╪.html	6	c54b90ceedeeb759a49ae02867eb6ae7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_1-1.html	2	f22f97924aec3a61103e98c8b98212f7
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_1-1_core.html	3	b2604153e5bb64eacb20320b59e5c20e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_1-2.html	2	b25a2c2ccc573f37997cf1dc951474d5
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_1-2_core.html	3	b2addd4c841d11b38363abdfe0f2cb05
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_2-1.html	2	8ed5707060e283d7407153c80cfe814a
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_2-1_core.html	2	248996c0a77c0bf79668f2c340fda647
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_2-2.html	2	7b3d060f0484d3f88468801ab2f6aac3
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_2-3.html	3	cb811428184328b446edfee985a890bf
/WebHallCMSV3.0BAProject/WebRoot/WEB-	3	8a2c9a8d04763eaafe1f8546ef922b5

INF/t/cms_sys_defined/style_list/style_2-4.html		e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_3-1.html	1	5d78f599ca89cdc070cf9af9e3fea053
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_3-1_core.html	3	100b32ae034e0079aae05e79e09226a1
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_3-2.html	1	febc502dafce0a0b2927a12e697ff027
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_list/style_3-3.html	1	c033846eb4c15dd91d0dea3ed9a59f48
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_page/channel_1.html	2	c0ef3914572064639b4ffdaf5bc4fe1f
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/t/cms_sys_defined/style_page/content_1.html	1	d41d8cd98f00b204e9800998ecf8427e
/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/web.xml	12	b0d9509702885e10cf1c86fe5ce31827

已扫描的查询

查询名称	找到的问题
Unsynchronized Access To Shared Data	2674
Unused Variable	2361
SQL Injection	2341
XSRF	2280
Input Not Normalized	2173
Heuristic SQL Injection	1883
Unnormalize Input String	1345
Incorrect Block Delimitation	895
Exposure of Resource to Wrong Sphere	827
Public Static Field Not Marked Final	626
CGI Reflected XSS All Clients	615
Potential O Reflected XSS All Clients	535
ESAPI Banned API	523
Trust Boundary Violation	522
Improper Exception Handling	389
Use of System Output Stream	360
Dead Code	356
Integer Underflow	355
Integer Overflow	353
Information Exposure Through an Error Message	295
Unchecked Input for Loop Condition	254
Divide By Zero	201
HTTP Response Splitting	186
Declaration Of Catch For Generic Exception	180

Dynamic SQL Queries	166
Reliance on Cookies in a Decision	166
Empty Methods	159
Declaration of Throws for Generic Exception	146
Client Potential XSS	128
Log Forging	126
Portability Flaw In File Separator	111
Absolute Path Traversal	110
Privacy Violation	107
Client Insecure Randomness	103
Input Path Not Canonicalized	98
CGI Stored XSS	88
Authorization Bypass Through User Controlled SQL PrimaryKey	84
Leftover Debug Code	70
Race Condition Format Flaw	69
Use of Obsolete Functions	64
Uncontrolled Recursion	62
Second Order SQL Injection	58
Client JQuery Deprecated Symbols	53
Client Potential DOM Open Redirect	51
Client Use Of Iframe Without Sandbox	51
Confusing Naming	50
Side Channel Data Leakage	50
Improper Resource Shutdown or Release	48
Insufficiently Protected Credentials	47
JSON Hijacking	46
Expression is Always False	41
Parameter Tampering	40
Detection of Error Condition Without Action	38
Unchecked Error Condition	38
Unclosed Objects	33
Race Condition	32
Reflected XSS All Clients	32
Stored Boundary Violation	31
Client Use Of JQuery Outdated Version	30
Data Leak Between Sessions	28
Use of Wrong Operator in String Comparison	28
Stored XSS	27
Exposure of System Data	24
Heuristic 2nd Order SQL Injection	24
Cleartext Submission of Sensitive Information	22
Potential Stored XSS	21
HttpOnlyCookies	20
Stored HTTP Response Splitting	20
Heuristic XSRF	19
Relative Path Traversal	17
Use of Cryptographically Weak PRNG	17
Use of Insufficiently Random Values	17
Client Potential Code Injection	16

Expression is Always True	16
Insufficient Transport Layer Protect	16
Failure to Catch All Exceptions in Servlet	14
Use Of Hardcoded Password	14
Not Static Final Logger	13
Serializable Class Containing Sensitive Data	13
Heuristic CGI Stored XSS	11
Stored Absolute Path Traversal	11
Cross Site History Manipulation	10
Public Static Final References Mutable Object	10
Uncontrolled Memory Allocation	9
Blind SQL Injections	8
Client DOM Open Redirect	8
Comparison of Classes By Name	8
Client DOM XSRF	7
Client DOM XSS	7
Heuristic Parameter Tampering	7
Heuristic Stored XSS	7
Malicious Program	7
Client Privacy Violation	6
Potentially Serializable Class With Sensitive Data	6
Stored Relative Path Traversal	6
Cookie Overly Broad Path	5
Missing Default Case In Switch Statement	5
Return Inside Finally Block	5
Reversible One Way Hash	5
Sensitive Cookie in HTTPS Session Without Secure Attribute	5
Stored Open Redirect	5
Missing XML Validation	4
Open Redirect	4
SQL Injection Evasion Attack	4
Use of Broken or Risky Cryptographic Algorithm	4
Use of Hard coded Cryptographic Key	4
Client DOM Cookie Poisoning	3
Client Password In Comment	3
Client ReDoS From Regex Injection	3
Client Remote File Inclusion	3
Client Server Empty Password	3
Hardcoded Connection String	3
Hardcoded password in Connection String	3
Improper Restriction of XXE Ref	3
Pages Without Global Error Handler	3
Stored Command Injection	3
Plaintext Storage in a Cookie	2
Weak Encryption	2
Access Specifier Manipulation	1
Catch NullPointerException	1
Client Regex Injection	1
Client Side ReDoS	1

Creation of Temp File in Dir with Incorrect Permissions	1
Creation of Temp File With Insecure Permissions	1
Direct Use of Threads	1
DoS by Sleep	1
HttpOnlyCookies In Config	1
Improper Initialization	1
Just One of Equals and Hash code Defined	1
Missing X Frame Options	1
Potential ReDoS	1
ReDoS In Pattern	1
Spring defaultHtmlEscape Not True	1
Uncaught Exception	1
Use of a One Way Hash without a Salt	1
Accessible Content Provider	0
Android Improper Resource Shutdown or Release	0
Array Declared Public Final and Static	0
Assigning instead of Comparing	0
Call to Thread run	0
Channel Accessible by NonEndpoint	0
Cleansing Canonicalization and Comparison Errors	0
Client Cookies Inspection	0
Client Cross Frame Scripting Attack	0
Client Cross Session Contamination	0
Client DB Parameter Tampering	0
Client DOM Code Injection	0
Client DOM Stored Code Injection	0
Client DOM Stored XSS	0
Client DoS By Sleep	0
Client Empty Password	0
Client Header Manipulation	0
Client HTML5 Heuristic Session Insecure Storage	0
Client HTML5 Information Exposure	0
Client HTML5 Insecure Storage	0
Client HTML5 Store Sensitive data In Web Storage	0
Client Insufficient ClickJacking Protection	0
Client Insufficient Key Size	0
Client Located JQuery Outdated Lib File	0
Client Negative Content Length	0
Client Overly Permissive Message Posting	0
Client Path Manipulation	0
Client Potential Ad Hoc Ajax	0
Client Potential ReDoS In Match	0
Client Potential ReDoS In Replace	0
Client ReDoS In Match	0
Client ReDos In RegExp	0
Client ReDoS In Replace	0
Client Resource Injection	0
Client Sandbox Allows Scripts With Same Origin	0
Client Second Order Sql Injection	0

Client Side Injection	0
Client SQL Injection	0
Client State Saving Method JSF	0
Client Untrusted Activex	0
Client Use Of Deprecated SQL Database	0
Client Weak Cryptographic Hash	0
Client Weak Encryption	0
Client Weak Password Authentication	0
Client XPATH Injection	0
clone Method Without super clone	0
Code Injection	0
Collapse of Data into Unsafe Value	0
Command Injection	0
Comparing instead of Assigning	0
Connection String Injection	0
Cookies Inspection	0
Critical Public Variable Without Final Modifier	0
Dangerous File Inclusion	0
DB Control of System or Config Setting	0
DB Parameter Tampering	0
Debuggable App	0
Direct Use of Sockets	0
Direct Use of Unsafe JNI	0
DOM Code Injection	0
DOM Cookie Poisoning	0
DOM Open Redirect	0
DOM XSRF	0
DOM XSS	0
Dynamic File Inclusion	0
Empty Password In Connection String	0
Empty Synchronized Block	0
ESAPI Same Password Repeats Twice	0
Escape False	0
Explicit Call to Finalize	0
Exported Service Without Permissions	0
Exposure Of Resource To Other Applications	0
External Control of Critical State Data	0
External Control of System or Config Setting	0
Failure To Implement Least Privilege	0
finalize Method Declared Public	0
finalize Method Without super finalize	0
General Android Find Request Permissions	0
GOTO Statement	0
GWT DOM XSS	0
GWT Reflected XSS	0
Hardcoded Absolute Path	0
Heuristic DB Parameter Tampering	0
Implicit Intent With Read Write Permissions	0
Improper Build Of Sql Mapping	0

Improper Locking	0
Improper Resource Locking	0
Improper Session Management	0
Improper Transaction Handling	0
Improper Verification Of Intent By Broadcast Receiver	0
Incorrect Conversion between Numeric Types	0
Information Exposure Through Debug Log	0
Information Exposure Through Server Log	0
Information Leak Through Comments	0
Information Leak Through Persistent Cookies	0
Information Leak Through Shell Error Message	0
Insecure Data Storage	0
Insecure WebView Usage	0
Insufficient Sensitive Transport Layer	0
Insufficient Session Expiration	0
LDAP Injection	0
Leaving Temporary File	0
Logic Time Bomb	0
Missing Password Field Masking	0
Multiple Binds to the Same Port	0
Non Encrypted Data Storage	0
Non serializable Object Stored in Session	0
Not Using a Random IV with CBC Mode	0
Null Pointer Dereference	0
Object Hijack	0
Off by One Error	0
Omitted Break Statement In Switch	0
Parse Double DoS	0
Passing Non Encrypted Data Between Activities	0
Path Traversal	0
Plaintext Storage of a Password	0
Poor Authorization and Authentication	0
Potential Code Injection	0
Potential Command Injection	0
Potential Connection String Injection	0
Potential GWT Reflected XSS	0
Potential I Reflected XSS All Clients	0
Potential IO Reflected XSS All Clients	0
Potential LDAP Injection	0
Potential Parameter Tampering	0
Potential ReDoS By Injection	0
Potential ReDoS In Match	0
Potential ReDoS In Replace	0
Potential ReDoS In Static Field	0
Potential Resource Injection	0
Potential SQL Injection	0
Potential UTF7 XSS	0
Potential XPath Injection	0
Potential XXE Injection	0

Process Control	0
Reachable Assertion	0
Redirect Without Exit	0
ReDoS From Regex Injection	0
ReDoS In Match	0
ReDoS In Replace	0
Reflected XSS	0
Reliance on Cookies without Validation	0
Reliance on DNS Lookups in a Decision	0
Resource Injection	0
Same Seed in PRNG	0
Session Fixation	0
Spring ModelView Injection	0
SSL Verification Bypass	0
Stored Code Injection	0
Stored LDAP Injection	0
Stored Path Traversal	0
Stored XPath Injection	0
Storing Passwords in a Recoverable Format	0
Struts Duplicate Config Files	0
Struts Duplicate Form Bean	0
Struts Duplicate Validation Files	0
Struts Duplicate Validation Forms	0
Struts Form Does Not Extend Validation Class	0
Struts Form Field Without Validator	0
Struts Incomplete Validate Method Definition	0
Struts Mapping to Missing Form Bean	0
Struts Missing Form Bean Name	0
Struts Missing Form Bean Type	0
Struts Missing Forward Name	0
Struts Non Private Field In ActionForm Class	0
Struts Thread Safety Violation In Action Class	0
Struts Unused Action Form	0
Struts Unused Validation Form	0
Struts Unvalidated Action Form	0
Struts Use of Relative Path in Config	0
Struts Validation Turned Off	0
Struts Validator Without Form Field	0
Struts2 Action Field Without Validator	0
Struts2 Duplicate Action Field Validators	0
Struts2 Duplicate Validators	0
Struts2 Undeclared Validator	0
Struts2 Validation File Without Action	0
Struts2 Validator Without Action Field	0
TOCTOU	0
Unchecked Return Value	0
Unchecked Return Value to NULL Pointer Dereference	0
Uncontrolled Format String	0
Unvalidated Forwards	0

Use of a One Way Hash with a Predictable Salt	0
Use of Client Side Authentication	0
Use of Deprecated or Obsolete Functions	0
Use Of getenv	0
Use of Hard coded Security Constants	0
Use Of Implicit Intent For Sensitive Communication	0
Use of Inner Class Containing Sensitive Data	0
Use of Native Language	0
Use of RSA Algorithm without OAEP	0
Use of System exit	0
Use Of Uninitialized Variables	0
Using Referer Field for Authentication	0
UTF7 XSS	0
VF Remoting Client Potential Code Injection	0
VF Remoting Client Potential XSRF	0
VF Remoting Client Potential XSS	0
Weak Password Authentication	0
XPath Injection	0

扫描结果细节

SQL Injection

描述

SQL Injection\路径 1021:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1021
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinesDaoImpl.java
行	182	200
对象	bsnum	executeUpdate

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
182.        public String save(String departmentid,String
permissionitemId,String bsnum,String createtime,
....
226.                    this.webhallBusinessMng.update(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebhallBusinessMngImpl.java

方法 public void update(String id){

```
....
48.   public void update(String id){
49.         this.dao.update(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinesDaoImpl.java

方法 public void update(String id){

```
....
198.        public void update(String id){
199.              String sql = "update TInsWebhallBusinessInfo bean set
bean.hasyy = '1' where bean.bsnum='"+id+"'";
200.              this.getSession().createQuery(sql).executeUpdate();
```

SQL Injection\路径 1022:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1022
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTagDaoImpl.java
行	575	118
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
575.              String bsnum = request.getParameter("bsnum");
....
578.              List<TInsLogTysp> list =
businessTagMng.findByBsnum(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/BusinessTagMngImpl.java

方法 public List<TInsLogTysp> findByBsnum(String bsnum) {

```
....
59.   public List<TInsLogTysp> findByBsnum(String bsnum) {
60.         return dao.findByBsnum(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTagDaoImpl.java

方法 public List<TInsLogTysp> findByBsnum(String bsnum) {

```
....
110.        public List<TInsLogTysp> findByBsnum(String bsnum) {
....
113.
      "nvl(operattype,'无'),nvl(isswap,'无'),nvl(nodetype,'无'),nvl(nodename,'无'),nvl(handlerid,'无'),nvl(nexthandlerid,'无') from tysp.t_ins_log where bsnum='"+bsnum+"'  order by arrivetime asc";
....
111.              String sql = "select nvl(lid,'无'),nvl(bsnum,'无'),nvl(flowid,'无'),nvl(nodeid,'无'),nvl(to_char(arrivetime, 'yyyy-MM-dd HH24:mm:ss'),'无') as arrivetime," +
....
118.              for(Object o: getSession().createSQLQuery(sql).list()){
```

SQL Injection\路径 1023:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1023
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTagDaoImpl.java
行	572	118
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {
....
575.              String bsnum = request.getParameter("bsnum");
....
578.              List<TInsLogTysp> list = businessTagMng.findByBsnum(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/BusinessTagMngImpl.java

方法 public List<TInsLogTysp> findByBsnum(String bsnum) {

```
....
59.   public List<TInsLogTysp> findByBsnum(String bsnum) {
60.         return dao.findByBsnum(bsnum);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BusinessTagDaoImpl.java
方法	public List<TInsLogTysp> findByBsnum(String bsnum) {

```
....
110.        public List<TInsLogTysp> findByBsnum(String bsnum) {
....
113.
      "nvl(operattype,'无'),nvl(isswap,'无'),nvl(nodetype,'无'),nvl(nodename,'无'),nvl(handlerid,'无'),nvl(nexthandlerid,'无') from tysp.t_ins_log where bsnum='"+bsnum+"'  order by arrivetime asc";
....
111.              String sql = "select nvl(lid,'无'),nvl(bsnum,'无'),nvl(flowid,'无'),nvl(nodeid,'无'),nvl(to_char(arrivetime, 'yyyy-MM-dd HH24:mm:ss'),'无') as arrivetime," +
....
118.              for(Object o: getSession().createSQLQuery(sql).list()){
```

SQL Injection\路径 1024:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1024
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	572	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
574.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1025:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1025
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	572	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
574.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1026:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1026
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	572	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
574.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1027:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1027
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	572	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
574.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1028:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1028
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	572	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Detail(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
572.        public String index4Detail(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
574.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1029:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1029
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	112	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
141.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1030:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1030
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	112	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
141.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1031:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1031
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	112	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
141.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1032:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1032
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
141.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1033:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1033
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
141.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1034:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1034
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	157	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
181.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1035:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1035
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	157	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
181.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1036:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1036
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	157	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
181.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1037:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1037
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	157	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
181.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1038:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1038
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	157	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
181.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1039:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1039
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	195	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
195.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String areaId,
....
221.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1040:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1040
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	195	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
195.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String areaId,
....
221.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1041:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1041
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	195	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
195.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String areaId,
....
221.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1042:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1042
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	195	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
195.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String areaId,
....
221.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1043:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1043
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	195	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
195.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String areaId,
....
221.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1044:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1044
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	237	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
237.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String areaId,
....
258.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1045:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1045
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	237	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
237.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String areaId,
....
258.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1046:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1046
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	237	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
237.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String areaId,
....
258.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1047:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1047
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	237	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
237.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String areaId,
....
258.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1048:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1048
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	237	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
237.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String areaId,
....
258.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1049:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1049
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	273	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
273.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
299.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1050:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1050
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	273	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
273.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
299.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1051:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1051
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	273	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
273.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
299.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1052:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1052
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	273	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
273.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
299.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1053:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1053
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	273	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
273.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
299.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1054:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1054
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	318	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
344.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1055:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1055
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	318	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
344.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1056:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1056
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	318	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
344.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1057:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1057
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	318	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
344.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1058:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1058
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	318	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
344.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1059:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1059
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	364	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
388.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1060:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1060
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	364	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
388.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1061:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1061
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	364	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
388.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1062:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1062
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	364	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
388.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1063:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1063
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	364	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
388.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1064:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1064
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	404	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
404.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
425.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1065:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1065
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	404	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
404.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
425.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1066:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1066
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	404	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
404.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
425.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1067:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1067
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	404	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
404.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
425.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1068:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1068
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	404	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
404.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
425.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1069:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1069
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	442	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
442.        public String getFavoriteByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
447.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1070:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1070
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	442	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
442.        public String getFavoriteByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
447.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1071:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1071
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	442	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
442.        public String getFavoriteByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
447.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1072:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1072
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	442	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
442.        public String getFavoriteByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
447.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1073:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1073
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	442	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
442.        public String getFavoriteByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
447.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1074:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1074
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	462	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
462.        public String getFavoriteGrByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
467.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1075:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1075
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	462	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
462.        public String getFavoriteGrByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
467.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1076:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1076
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	462	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
462.        public String getFavoriteGrByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
467.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1077:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1077
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	462	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
462.        public String getFavoriteGrByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
467.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1078:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1078
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	462	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
462.        public String getFavoriteGrByUser(String username,String
areaId,HttpServletRequest request, ModelMap model){
....
467.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1079:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1079
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	106	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
138.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1080:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1080
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	106	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
138.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1081:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1081
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	106	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
138.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1082:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1082
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
138.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1083:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1083
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
138.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1084:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1084
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	153	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
177.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1085:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1085
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	153	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
177.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1086:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1086
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	153	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
177.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1087:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1087
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	153	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
177.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1088:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1088
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	153	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
177.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1089:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1089
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	191	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
191.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
217.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1090:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1090
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	191	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
191.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
217.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1091:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1091
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	191	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
191.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
217.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1092:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1092
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	191	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
191.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
217.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1093:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1093
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	191	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
191.        public String enterpriseDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
217.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1094:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1094
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	233	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
233.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
254.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1095:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1095
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	233	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
233.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
254.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1096:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1096
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	233	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
233.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
254.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1097:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1097
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	233	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
233.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
254.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1098:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1098
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	233	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
233.        public String enterpriseDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
254.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1099:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1099
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	269	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
269.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
295.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1100:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1100
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	269	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
269.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
295.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1101:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1101
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	269	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
269.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
295.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1102:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1102
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	269	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
269.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
295.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1103:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1103
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	269	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
269.        public String enterpriseSsDeptStorePermBySxid(String
sxid,String sxzxname,String sortcode,String areaId,
....
295.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1104:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1104
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	312	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
312.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
333.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1105:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1105
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	312	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
312.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
333.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1106:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1106
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	312	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
312.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
333.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1107:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1107
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	312	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
312.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
333.                request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1108:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1108
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	312	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
312.        public String enterpriseSsDeptCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String areaId,
....
333.              request.setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1109:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1109
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	195	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String input(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
195.        public String input(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
197.                String info = request.getParameter("info");
198.                String loginto = request.getParameter("loginto");
....
305.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1110:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1110
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	195	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String input(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
195.        public String input(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
197.                String info = request.getParameter("info");
198.                String loginto = request.getParameter("loginto");
....
305.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1111:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1111
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	195	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String input(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
195.        public String input(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
197.                String info = request.getParameter("info");
198.                String loginto = request.getParameter("loginto");
....
305.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1112:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1112
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	195	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String input(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
195.        public String input(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
197.              String info = request.getParameter("info");
198.              String loginto = request.getParameter("loginto");
....
305.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1113:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1113
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	195	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String input(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
195.        public String input(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
197.                String info = request.getParameter("info");
198.                String loginto = request.getParameter("loginto");
....
305.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1114:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1114
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	96	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1115:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1115
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	96	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1116:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1116
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	96	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1117:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1117
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1118:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1118
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1119:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1119
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	221	37
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index2(String areaId, String stab,

```
....
221.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
223.                String region = request.getParameter("region");
224.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
227.                String selectTagNo =
request.getParameter("selectTagNo");
....
229.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
381.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
400.                request.getSession().setAttribute("zcjianFlg", "1");
401.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1120:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1120
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	221	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String index2(String areaId, String stab,

```
....
221.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
223.                String region = request.getParameter("region");
224.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
227.                String selectTagNo =
request.getParameter("selectTagNo");
....
229.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
381.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
400.                request.getSession().setAttribute("zcjianFlg", "1");
401.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1121:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1121
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	221	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index2(String areaId, String stab,

```
....
221.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
223.                String region = request.getParameter("region");
224.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
227.                String selectTagNo =
request.getParameter("selectTagNo");
....
229.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
381.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
400.                request.getSession().setAttribute("zcjianFlg", "1");
401.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1122:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1122
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	221	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index2(String areaId, String stab,

```
....
221.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
223.                String region = request.getParameter("region");
224.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
227.                String selectTagNo =
request.getParameter("selectTagNo");
....
229.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
381.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
400.                request.getSession().setAttribute("zcjianFlg", "1");
401.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1123:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1123
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	221	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index2(String areaId, String stab,

```
....
221.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
223.                String region = request.getParameter("region");
224.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
227.                String selectTagNo =
request.getParameter("selectTagNo");
....
229.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
381.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
400.                request.getSession().setAttribute("zcjianFlg", "1");
401.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1124:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1124
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	419	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index(HttpServletRequest request,

```
....
419.        public String index(HttpServletRequest request,
....
425.                String selectTagNo =
request.getParameter("selectTagNo");
....
428.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1125:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1125
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	419	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String index(HttpServletRequest request,

```
....
419.        public String index(HttpServletRequest request,
....
425.              String selectTagNo =
request.getParameter("selectTagNo");
....
428.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1126:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1126
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	419	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String index(HttpServletRequest request,

```
....
419.        public String index(HttpServletRequest request,
....
425.                String selectTagNo =
request.getParameter("selectTagNo");
....
428.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1127:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1127
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	419	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String index(HttpServletRequest request,

```
....
419.        public String index(HttpServletRequest request,
....
425.                String selectTagNo =
request.getParameter("selectTagNo");
....
428.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1128:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1128
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	419	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String index(HttpServletRequest request,

```
....
419.        public String index(HttpServletRequest request,
....
425.                String selectTagNo =
request.getParameter("selectTagNo");
....
428.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1129:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1129
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	465	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
465.        public String profileInput(HttpServletRequest request,
....
473.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1130:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1130
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	465	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
465.        public String profileInput(HttpServletRequest request,
....
473.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1131:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1131
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	465	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
465.        public String profileInput(HttpServletRequest request,
....
473.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1132:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1132
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	465	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
465.        public String profileInput(HttpServletRequest request,
....
473.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1133:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1133
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	465	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
465.        public String profileInput(HttpServletRequest request,
....
473.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1134:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1134
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	498	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
498.                    HttpServletRequest request, HttpServletResponse
response,
....
509.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1135:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1135
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	498	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
498.                    HttpServletRequest request, HttpServletResponse
response,
....
509.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1136:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1136
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	498	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
498.                    HttpServletRequest request, HttpServletResponse
response,
....
509.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1137:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1137
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	498	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
498.                    HttpServletRequest request, HttpServletResponse
response,
....
509.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1138:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1138
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	498	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
498.                    HttpServletRequest request, HttpServletResponse
response,
....
509.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1139:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1139
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	604	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
613.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1140:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1140
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	604	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
613.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1141:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1141
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	604	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
613.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1142:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1142
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	604	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
613.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1143:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1143
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	604	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
613.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1144:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1144
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	637	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
637.                    String nextUrl, HttpServletRequest request,
....
658.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1145:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1145
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	637	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
637.                    String nextUrl, HttpServletRequest request,
....
658.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1146:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1146
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	637	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
637.                    String nextUrl, HttpServletRequest request,
....
658.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1147:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1147
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	637	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
637.                    String nextUrl, HttpServletRequest request,
....
658.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1148:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1148
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	637	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
637.                    String nextUrl, HttpServletRequest request,
....
658.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1149:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1149
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	96	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1150:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1150
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	96	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1151:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1151
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	96	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1152:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1152
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1153:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1153
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
96.   public String input(HttpServletRequest request, ModelMap model) {
....
129.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1154:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1154
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	223	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index2(String areaId, String stab,

```
....
223.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
225.                String region = request.getParameter("region");
226.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
229.                String selectTagNo =
request.getParameter("selectTagNo");
....
231.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
364.                request.getSession().setAttribute("zcjianFlg", "1");
....
368.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1155:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1155
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	223	241
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index2(String areaId, String stab,

```
....
223.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
225.                String region = request.getParameter("region");
226.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
229.                String selectTagNo =
request.getParameter("selectTagNo");
....
231.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
364.                request.getSession().setAttribute("zcjianFlg", "1");
....
368.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1156:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1156
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	223	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index2(String areaId, String stab,

```
....
223.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
225.                String region = request.getParameter("region");
226.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
229.                String selectTagNo =
request.getParameter("selectTagNo");
....
231.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
364.                request.getSession().setAttribute("zcjianFlg", "1");
....
368.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1157:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1157
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	223	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index2(String areaId, String stab,

```
....
223.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
225.                String region = request.getParameter("region");
226.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
229.                String selectTagNo =
request.getParameter("selectTagNo");
....
231.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
364.                request.getSession().setAttribute("zcjianFlg", "1");
....
368.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1158:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1158
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	223	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index2(String areaId, String stab,

```
....
223.                    HttpServletRequest request,HttpServletResponse
response,Integer pageNo,  ModelMap model) {
....
225.                String region = request.getParameter("region");
226.                String cid = request.getParameter("cid");//
从事项列表和事项列表_姓名点击进入
....
229.                String selectTagNo =
request.getParameter("selectTagNo");
....
231.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.
      if("1".equals(request.getSession().getAttribute("zcjianFlg"))){
....
364.                request.getSession().setAttribute("zcjianFlg", "1");
....
368.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1159:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1159
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	432	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String profileInput(HttpServletRequest request,

```
....
432.        public String profileInput(HttpServletRequest request,
....
440.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1160:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1160
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	432	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String profileInput(HttpServletRequest request,

```
....
432.        public String profileInput(HttpServletRequest request,
....
440.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1161:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1161
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	432	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileInput(HttpServletRequest request,

```
....
432.        public String profileInput(HttpServletRequest request,
....
440.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1162:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1162
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	432	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileInput(HttpServletRequest request,

```
....
432.        public String profileInput(HttpServletRequest request,
....
440.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1163:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1163
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	432	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileInput(HttpServletRequest request,

```
....
432.        public String profileInput(HttpServletRequest request,
....
440.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1164:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1164
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	675	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
675.                    String nextUrl, HttpServletRequest request,
....
699.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1165:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1165
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	675	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
675.                    String nextUrl, HttpServletRequest request,
....
699.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1166:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1166
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	675	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
675.                    String nextUrl, HttpServletRequest request,
....
699.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1167:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1167
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	675	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
675.                    String nextUrl, HttpServletRequest request,
....
699.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1168:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1168
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	675	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
675.                    String nextUrl, HttpServletRequest request,
....
699.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1169:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1169
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	465	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
465.                    HttpServletRequest request, HttpServletResponse
response,
....
476.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1170:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1170
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	465	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
465.                    HttpServletRequest request, HttpServletResponse
response,
....
476.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1171:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1171
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	465	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
465.                    HttpServletRequest request, HttpServletResponse
response,
....
476.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1172:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1172
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	465	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
465.                    HttpServletRequest request, HttpServletResponse
response,
....
476.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1173:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1173
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	465	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
465.                    HttpServletRequest request, HttpServletResponse
response,
....
476.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1174:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1174
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	604	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
626.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1175:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1175
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	604	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
626.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1176:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1176
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	604	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
626.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1177:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1177
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	604	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
626.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1178:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1178
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	604	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingPhoneSubmit(String phoneNumber,

```
....
604.                    String nextUrl, HttpServletRequest request,
....
626.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1179:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1179
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	643	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
643.                    String nextUrl, HttpServletRequest request,
....
668.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1180:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1180
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	643	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
643.                    String nextUrl, HttpServletRequest request,
....
668.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1181:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1181
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	643	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
643.                    String nextUrl, HttpServletRequest request,
....
668.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1182:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1182
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	643	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
643.                    String nextUrl, HttpServletRequest request,
....
668.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1183:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1183
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	643	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String bindingEmailSubmit(String bindingEmail,

```
....
643.                    String nextUrl, HttpServletRequest request,
....
668.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1184:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1184
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	724	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordInput(HttpServletRequest request,

```
....
724.        public String passwordInput(HttpServletRequest request,
....
732.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1185:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1185
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	724	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordInput(HttpServletRequest request,

```
....
724.        public String passwordInput(HttpServletRequest request,
....
732.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1186:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1186
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	724	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordInput(HttpServletRequest request,

```
....
724.        public String passwordInput(HttpServletRequest request,
....
732.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1187:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1187
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	724	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordInput(HttpServletRequest request,

```
....
724.        public String passwordInput(HttpServletRequest request,
....
732.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1188:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1188
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	724	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordInput(HttpServletRequest request,

```
....
724.        public String passwordInput(HttpServletRequest request,
....
732.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1189:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1189
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	105	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
105.        public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
110.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
120.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1190:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1190
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	105	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
105.        public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
110.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
120.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1191:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1191
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	105	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
105.        public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
110.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
120.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1192:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1192
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	105	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
105.        public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
110.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
120.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1193:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1193
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	105	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
105.        public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
110.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
120.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1194:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1194
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	213	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
213.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
216.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
219.              String selectTagNo =
request.getParameter("selectTagNo");
220.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
221.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
222.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
233.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1195:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1195
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	213	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
213.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
216.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
219.              String selectTagNo =
request.getParameter("selectTagNo");
220.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
221.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
222.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
233.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1196:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1196
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	213	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
213.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
216.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
219.              String selectTagNo =
request.getParameter("selectTagNo");
220.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
221.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
222.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
233.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1197:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1197
结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	213	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
213.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
216.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
219.              String selectTagNo =
request.getParameter("selectTagNo");
220.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
221.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
222.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
233.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1198:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1198
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	213	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
213.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
216.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
219.              String selectTagNo =
request.getParameter("selectTagNo");
220.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
221.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
222.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
233.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1199:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1199
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	386	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String index(HttpServletRequest request,

```
....
386.        public String index(HttpServletRequest request,
....
392.                String selectTagNo =
request.getParameter("selectTagNo");
....
395.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1200:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1200
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	386	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String index(HttpServletRequest request,

```
....
386.        public String index(HttpServletRequest request,
....
392.                String selectTagNo =
request.getParameter("selectTagNo");
....
395.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1201:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1201
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	386	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index(HttpServletRequest request,

```
....
386.        public String index(HttpServletRequest request,
....
392.                String selectTagNo =
request.getParameter("selectTagNo");
....
395.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1202:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1202
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	386	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index(HttpServletRequest request,

```
....
386.        public String index(HttpServletRequest request,
....
392.                String selectTagNo =
request.getParameter("selectTagNo");
....
395.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1203:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1203
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	386	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String index(HttpServletRequest request,

```
....
386.        public String index(HttpServletRequest request,
....
392.                String selectTagNo =
request.getParameter("selectTagNo");
....
395.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1204:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1204
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	316	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
316.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
321.                String selectTagNo =
request.getParameter("selectTagNo");
....
324.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1205:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1205
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	316	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
316.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
321.                String selectTagNo =
request.getParameter("selectTagNo");
....
324.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1206:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1206
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	316	272
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
316.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
321.                String selectTagNo =
request.getParameter("selectTagNo");
....
324.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1207:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1207
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	316	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
316.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
321.                String selectTagNo =
request.getParameter("selectTagNo");
....
324.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1208:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1208
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	316	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
316.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
321.                String selectTagNo =
request.getParameter("selectTagNo");
....
324.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1209:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1209
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	398	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String listPermBySort(String sortcode,

```
....
398.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
401.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
407.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1210:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1210
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	398	241
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String listPermBySort(String sortcode,

```
....
398.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
401.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
407.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1211:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1211
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	398	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String listPermBySort(String sortcode,

```
....
398.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
401.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
407.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1212:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1212
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	398	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String listPermBySort(String sortcode,

```
....
398.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
401.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
407.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1213:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1213
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	398	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String listPermBySort(String sortcode,

```
....
398.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
401.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
407.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1214:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1214
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	755	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String passwordInput(HttpServletRequest request,

```
....
755.        public String passwordInput(HttpServletRequest request,
....
763.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1215:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1215
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	755	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
755.        public String passwordInput(HttpServletRequest request,
....
763.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1216:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1216
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	755	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
755.        public String passwordInput(HttpServletRequest request,
....
763.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1217:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1217
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	755	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
755.        public String passwordInput(HttpServletRequest request,
....
763.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1218:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1218
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	755	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
755.        public String passwordInput(HttpServletRequest request,
....
763.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1219:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1219
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	571	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
571.                    String nextUrl, HttpServletRequest request,
....
580.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1220:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1220
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	571	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
571.                    String nextUrl, HttpServletRequest request,
....
580.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1221:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1221
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	571	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
571.                    String nextUrl, HttpServletRequest request,
....
580.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1222:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1222
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	571	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
571.                    String nextUrl, HttpServletRequest request,
....
580.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1223:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1223
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	571	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
571.                    String nextUrl, HttpServletRequest request,
....
580.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1224:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1224
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	494	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String list(String deptid, String permtype,

```
....
494.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
508.                deptid =
request.getSession().getAttribute("deptId")+"";
....
511.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1225:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1225
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	494	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String list(String deptid, String permtype,

```
....
494.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
508.              deptid =
request.getSession().getAttribute("deptId")+"";
....
511.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1226:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1226
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	494	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String list(String deptid, String permtype,

```
....
494.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
508.              deptid =
request.getSession().getAttribute("deptId")+"";
....
511.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1227:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1227
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	494	218
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String list(String deptid, String permtype,

```
....
494.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
508.              deptid =
request.getSession().getAttribute("deptId")+"";
....
511.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1228:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1228
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	494	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String list(String deptid, String permtype,

```
....
494.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
508.              deptid =
request.getSession().getAttribute("deptId")+"";
....
511.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1229:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1229
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	584	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String banshitingpingjia(HttpServletRequest request,

```
....
584.        public String banshitingpingjia(HttpServletRequest request,
....
587.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1230:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1230
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	584	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
584.        public String banshitingpingjia(HttpServletRequest request,
....
587.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1231:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1231
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	584	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
584.        public String banshitingpingjia(HttpServletRequest request,
....
587.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1232:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1232
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	584	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingpingjia(HttpServletRequest request,

```
....
584.        public String banshitingpingjia(HttpServletRequest request,
....
587.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1233:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1233
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	584	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
584.        public String banshitingpingjia(HttpServletRequest request,
....
587.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1234:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1234
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	656	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
664.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
667.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1235:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1235
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	656	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
681.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1236:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1236
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	656	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
681.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1237:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1237
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	656	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
664.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
667.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1238:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1238
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	656	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
664.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
667.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1239:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1239
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	656	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
664.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
667.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1240:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1240
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	656	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
656.        public String done(HttpServletRequest request,
....
660.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
664.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
667.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1241:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1241
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	692	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
703.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1242:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1242
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	692	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
716.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1243:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1243
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	692	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
716.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1244:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1244
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	692	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
703.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1245:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1245
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	692	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
703.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1246:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1246
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	692	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
703.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1247:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1247
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	692	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
692.        public String temporary(HttpServletRequest request,
....
696.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
698.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
703.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1248:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1248
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	801	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String complain(HttpServletRequest request,

```
....
801.        public String complain(HttpServletRequest request,
....
805.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
810.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1249:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1249
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	801	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String complain(HttpServletRequest request,

```
....
801.        public String complain(HttpServletRequest request,
....
805.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
810.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1250:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1250
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	801	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String complain(HttpServletRequest request,

```
....
801.        public String complain(HttpServletRequest request,
....
805.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
810.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1251:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1251
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	801	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String complain(HttpServletRequest request,

```
....
801.        public String complain(HttpServletRequest request,
....
805.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
810.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1252:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1252
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	801	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String complain(HttpServletRequest request,

```
....
801.        public String complain(HttpServletRequest request,
....
805.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
810.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1253:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1253
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	835	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String suggest(HttpServletRequest request,

```
....
835.        public String suggest(HttpServletRequest request,
....
839.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
844.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1254:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1254
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	835	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String suggest(HttpServletRequest request,

```
....
835.        public String suggest(HttpServletRequest request,
....
839.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
844.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1255:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1255
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	835	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String suggest(HttpServletRequest request,

```
....
835.        public String suggest(HttpServletRequest request,
....
839.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
844.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1256:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1256
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	835	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String suggest(HttpServletRequest request,

```
....
835.        public String suggest(HttpServletRequest request,
....
839.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
844.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1257:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1257
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	835	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String suggest(HttpServletRequest request,

```
....
835.        public String suggest(HttpServletRequest request,
....
839.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
844.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1258:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1258
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	870	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String online(HttpServletRequest request,

```
....
870.        public String online(HttpServletRequest request,
....
874.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
879.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1259:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1259
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	870	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String online(HttpServletRequest request,

```
....
870.        public String online(HttpServletRequest request,
....
874.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
879.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1260:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1260
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	870	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String online(HttpServletRequest request,

```
....
870.        public String online(HttpServletRequest request,
....
874.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
879.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1261:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1261
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	870	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String online(HttpServletRequest request,

```
....
870.        public String online(HttpServletRequest request,
....
874.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
879.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1262:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1262
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	870	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String online(HttpServletRequest request,

```
....
870.        public String online(HttpServletRequest request,
....
874.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
879.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1263:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1263
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1006	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String collection(HttpServletRequest request,

```
....
1006.       public String collection(HttpServletRequest request,
....
1010.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1015.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1264:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1264
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1006	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String collection(HttpServletRequest request,

```
....
1006.       public String collection(HttpServletRequest request,
....
1010.             UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1015.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1265:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1265
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1006	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String collection(HttpServletRequest request,

```
....
1006.       public String collection(HttpServletRequest request,
....
1010.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1015.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1266:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1266
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1006	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String collection(HttpServletRequest request,

```
....
1006.       public String collection(HttpServletRequest request,
....
1010.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1015.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1267:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1267
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1006	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String collection(HttpServletRequest request,

```
....
1006.       public String collection(HttpServletRequest request,
....
1010.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1015.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1268:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1268
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	458	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
458.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
475.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1269:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1269
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	458	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
458.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
475.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1270:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1270
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	458	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
458.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
475.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1271:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1271
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	458	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
458.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
475.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1272:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1272
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	458	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
458.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
475.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1273:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1273
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1054	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String nformation(HttpServletRequest request,

```
....
1054.       public String nformation(HttpServletRequest request,
....
1058.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1063.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1274:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1274
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1054	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String nformation(HttpServletRequest request,

```
....
1054.       public String nformation(HttpServletRequest request,
....
1058.             UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1063.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1275:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1275
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1054	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String nformation(HttpServletRequest request,

```
....
1054.       public String nformation(HttpServletRequest request,
....
1058.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1063.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1276:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1276
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1054	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String nformation(HttpServletRequest request,

```
....
1054.       public String nformation(HttpServletRequest request,
....
1058.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1063.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1277:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1277
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1054	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String nformation(HttpServletRequest request,

```
....
1054.       public String nformation(HttpServletRequest request,
....
1058.               UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
1063.                   return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1278:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1278
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	618	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
630.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1279:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1279
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	618	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
645.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1280:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1280
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	618	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
645.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1281:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1281
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	618	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
630.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1282:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1282
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	618	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
630.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1283:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1283
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	618	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
630.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1284:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1284
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	618	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
618.        public String todo(HttpServletRequest request,
....
622.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
625.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
630.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1285:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1285
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	89	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
89.   public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
96.         UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
103.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1286:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1286
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	89	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
89.   public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
96.         UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
103.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1287:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1287
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	89	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
89.   public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
96.         UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
103.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1288:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1288
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	89	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
89.   public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
96.         UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
103.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1289:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1289
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	89	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndex(HttpServletRequest request,HttpServletResponse response,

```
....
89.   public String banshitingIndex(HttpServletRequest
request,HttpServletResponse response,
....
96.         UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
103.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1290:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1290
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	189	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
189.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
193.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
195.              String selectTagNo =
request.getParameter("selectTagNo");
196.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
197.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
198.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1291:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1291
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	189	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
189.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
193.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
195.              String selectTagNo =
request.getParameter("selectTagNo");
196.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
197.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
198.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1292:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1292
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	189	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
189.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
193.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
195.              String selectTagNo =
request.getParameter("selectTagNo");
196.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
197.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
198.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1293:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1293
结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	189	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
189.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
193.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
195.              String selectTagNo =
request.getParameter("selectTagNo");
196.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
197.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
198.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1294:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1294
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	189	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingIndexPOST(HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {

```
....
189.        public String banshitingIndexPOST(HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo,Integer pageNoBJ,ModelMap model) {
....
193.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
195.              String selectTagNo =
request.getParameter("selectTagNo");
196.              String selectTagNoBJ =
request.getParameter("selectTagNoBJ");
197.              String selectTagNoFW =
request.getParameter("selectTagNoFW");
198.              String selectTagNoTS =
request.getParameter("selectTagNoTS");
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1295:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1295
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	766	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String consult(HttpServletRequest request,

```
....
766.        public String consult(HttpServletRequest request,
....
770.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
775.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1296:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1296
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	766	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String consult(HttpServletRequest request,

```
....
766.        public String consult(HttpServletRequest request,
....
770.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
775.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1297:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1297
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	766	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String consult(HttpServletRequest request,

```
....
766.        public String consult(HttpServletRequest request,
....
770.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
775.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1298:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1298
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	766	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String consult(HttpServletRequest request,

```
....
766.        public String consult(HttpServletRequest request,
....
770.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
775.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1299:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1299
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	766	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String consult(HttpServletRequest request,

```
....
766.        public String consult(HttpServletRequest request,
....
770.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
775.                        return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1300:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1300
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	293	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
293.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
298.                String selectTagNo =
request.getParameter("selectTagNo");
....
301.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1301:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1301
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	293	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
293.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
298.                String selectTagNo =
request.getParameter("selectTagNo");
....
301.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1302:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1302
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	293	272
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
293.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
298.                String selectTagNo =
request.getParameter("selectTagNo");
....
301.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1303:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1303
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	293	218
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
293.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
298.                String selectTagNo =
request.getParameter("selectTagNo");
....
301.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1304:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1304
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	293	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String enterpriseCancellationOfFWSC(String sxid,String sxzxname,String fcode,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model){

```
....
293.        public String enterpriseCancellationOfFWSC(String
sxid,String sxzxname,String fcode,HttpServletRequest
request,HttpServletResponse response,Integer pageNoWXTS,Integer
pageNoFWSC,Integer pageNo, ModelMap model){
....
298.                String selectTagNo =
request.getParameter("selectTagNo");
....
301.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1305:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1305
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	374	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String listPermBySort(String sortcode,

```
....
374.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
377.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1306:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1306
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	374	241
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String listPermBySort(String sortcode,

```
....
374.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
377.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1307:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1307
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	374	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String listPermBySort(String sortcode,

```
....
374.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
377.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1308:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1308
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	374	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String listPermBySort(String sortcode,

```
....
374.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
377.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1309:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1309
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	374	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String listPermBySort(String sortcode,

```
....
374.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
377.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1310:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1310
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	433	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String ajax_listPermBySortsc(String sortcode,

```
....
433.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
435.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1311:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1311
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	433	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String ajax_listPermBySortsc(String sortcode,

```
....
433.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
435.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1312:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1312
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	433	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String ajax_listPermBySortsc(String sortcode,

```
....
433.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
435.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1313:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1313
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	433	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String ajax_listPermBySortsc(String sortcode,

```
....
433.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
435.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1314:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1314
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	433	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String ajax_listPermBySortsc(String sortcode,

```
....
433.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
435.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1315:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1315
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	496	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
496.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
513.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1316:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1316
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	496	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
496.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
513.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1317:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1317
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	496	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
496.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
513.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1318:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1318
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	496	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
496.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
513.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1319:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1319
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	496	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
496.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
513.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1320:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1320
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	532	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String list(String deptid, String permtype,

```
....
532.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
546.                deptid =
request.getSession().getAttribute("deptId")+"";
....
549.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1321:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1321
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	532	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String list(String deptid, String permtype,

```
....
532.                     Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
546.               deptid =
request.getSession().getAttribute("deptId")+"";
....
549.                     FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1322:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1322
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	532	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String list(String deptid, String permtype,

```
....
532.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
546.              deptid =
request.getSession().getAttribute("deptId")+"";
....
549.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1323:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1323
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	532	218
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String list(String deptid, String permtype,

```
....
532.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
546.                deptid =
request.getSession().getAttribute("deptId")+"";
....
549.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1324:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1324
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	532	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String list(String deptid, String permtype,

```
....
532.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
546.              deptid =
request.getSession().getAttribute("deptId")+"";
....
549.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1325:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1325
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	622	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingpingjia(HttpServletRequest request,

```
....
622.        public String banshitingpingjia(HttpServletRequest request,
....
625.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1326:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1326
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	622	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
622.        public String banshitingpingjia(HttpServletRequest request,
....
625.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1327:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1327
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	622	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
622.        public String banshitingpingjia(HttpServletRequest request,
....
625.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1328:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1328
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	622	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingpingjia(HttpServletRequest request,

```
....
622.        public String banshitingpingjia(HttpServletRequest request,
....
625.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1329:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1329
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	622	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingpingjia(HttpServletRequest request,

```
....
622.        public String banshitingpingjia(HttpServletRequest request,
....
625.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1330:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1330
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	658	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
661.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1331:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1331
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	658	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
673.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
679.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.                sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.                Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.                querycount.setCacheable(false);
133.                List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.                return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                        buf.append(c);
....
827.                        buf.append("[%]");
....
824.                        buf.append("[_]");
....
821.                        buf.append("[[]");
....
818.                        buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1332:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1332

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	658	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
673.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
679.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.                sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.                sb.append(") tv)R WHERE R.RNUM>");
160.                sb.append((pageNo-1)*pageSize);
161.                sb.append(" AND R.RNUM<=");
162.                sb.append(pageNo*pageSize);
163.                Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.                query.setCacheable(false);
165.                List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1333:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1333
结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	658	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
661.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1334:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1334
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	658	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
661.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1335:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1335
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	658	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
661.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1336:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1336
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	658	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
658.        public String todo(HttpServletRequest request,
....
661.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1337:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1337
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	690	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
693.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1338:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1338
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	690	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
705.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
709.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.                sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.                Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.                querycount.setCacheable(false);
133.                List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1339:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1339

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	690	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
705.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
709.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.                sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.                sb.append(") tv)R WHERE R.RNUM>");
160.                sb.append((pageNo-1)*pageSize);
161.                sb.append(" AND R.RNUM<=");
162.                sb.append(pageNo*pageSize);
163.                Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.                query.setCacheable(false);
165.                List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.                return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                        buf.append(c);
....
821.                        buf.append("[[]");
....
818.                        buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1340:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1340
结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	690	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
693.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1341:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1341
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	690	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
693.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1342:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1342
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	690	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
693.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1343:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1343
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	690	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
690.        public String done(HttpServletRequest request,
....
693.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1344:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1344
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	720	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
723.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1345:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1345
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	720	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
735.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
739.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.                sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.                Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.                querycount.setCacheable(false);
133.                List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.                return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                        buf.append(c);
....
827.                        buf.append("[%]");
....
824.                        buf.append("[_]");
....
821.                        buf.append("[[]");
....
818.                        buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1346:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1346

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	720	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
735.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
739.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.                sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.                sb.append(") tv)R WHERE R.RNUM>");
160.                sb.append((pageNo-1)*pageSize);
161.                sb.append(" AND R.RNUM<=");
162.                sb.append(pageNo*pageSize);
163.                Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.                query.setCacheable(false);
165.                List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.                return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                        buf.append(c);
....
821.                        buf.append("[[]");
....
818.                        buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1347:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1347
结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	720	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
723.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1348:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1348
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	720	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
723.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1349:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1349
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	720	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
723.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1350:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1350
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	720	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
720.        public String temporary(HttpServletRequest request,
....
723.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1351:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1351
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	751	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1352:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1352
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	751	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
766.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
770.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.                sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.                Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.                querycount.setCacheable(false);
133.                List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1353:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1353

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	751	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
766.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
770.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.                sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.                sb.append(") tv)R WHERE R.RNUM>");
160.                sb.append((pageNo-1)*pageSize);
161.                sb.append(" AND R.RNUM<=");
162.                sb.append(pageNo*pageSize);
163.                Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.                query.setCacheable(false);
165.                List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.                return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                        buf.append(c);
....
821.                        buf.append("[[]");
....
818.                        buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1354:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1354
结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	751	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1355:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1355
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	751	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1356:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1356
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	751	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1357:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1357
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	751	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
751.        public String back(HttpServletRequest request,
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1358:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1358
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	783	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String consult(HttpServletRequest request,

```
....
783.        public String consult(HttpServletRequest request,
....
786.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1359:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1359
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	783	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String consult(HttpServletRequest request,

```
....
783.        public String consult(HttpServletRequest request,
....
786.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1360:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1360
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	783	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String consult(HttpServletRequest request,

```
....
783.        public String consult(HttpServletRequest request,
....
786.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1361:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1361
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	783	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String consult(HttpServletRequest request,

```
....
783.        public String consult(HttpServletRequest request,
....
786.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1362:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1362
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	783	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String consult(HttpServletRequest request,

```
....
783.        public String consult(HttpServletRequest request,
....
786.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1363:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1363
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	812	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String complain(HttpServletRequest request,

```
....
812.        public String complain(HttpServletRequest request,
....
815.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1364:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1364
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	812	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String complain(HttpServletRequest request,

```
....
812.        public String complain(HttpServletRequest request,
....
815.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1365:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1365
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	812	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String complain(HttpServletRequest request,

```
....
812.        public String complain(HttpServletRequest request,
....
815.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1366:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1366
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	812	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String complain(HttpServletRequest request,

```
....
812.        public String complain(HttpServletRequest request,
....
815.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1367:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1367
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	812	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String complain(HttpServletRequest request,

```
....
812.        public String complain(HttpServletRequest request,
....
815.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1368:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1368
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	840	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String suggest(HttpServletRequest request,

```
....
840.        public String suggest(HttpServletRequest request,
....
843.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1369:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1369
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	840	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String suggest(HttpServletRequest request,

```
....
840.        public String suggest(HttpServletRequest request,
....
843.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1370:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1370
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	840	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String suggest(HttpServletRequest request,

```
....
840.        public String suggest(HttpServletRequest request,
....
843.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1371:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1371
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	840	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String suggest(HttpServletRequest request,

```
....
840.        public String suggest(HttpServletRequest request,
....
843.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1372:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1372
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	840	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String suggest(HttpServletRequest request,

```
....
840.        public String suggest(HttpServletRequest request,
....
843.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1373:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1373
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	728	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1374:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1374
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	728	133
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
753.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1375:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1375
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	728	165
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
753.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 1376:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1376
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	728	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1377:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1377
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	728	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1378:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1378
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	728	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1379:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1379
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	728	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
728.        public String back(HttpServletRequest request,
....
732.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1380:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1380
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	869	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String online(HttpServletRequest request,

```
....
869.        public String online(HttpServletRequest request,
....
872.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1381:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1381
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	869	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String online(HttpServletRequest request,

```
....
869.        public String online(HttpServletRequest request,
....
872.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1382:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1382
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	869	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String online(HttpServletRequest request,

```
....
869.        public String online(HttpServletRequest request,
....
872.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1383:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1383
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	869	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String online(HttpServletRequest request,

```
....
869.        public String online(HttpServletRequest request,
....
872.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1384:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1384
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	869	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String online(HttpServletRequest request,

```
....
869.        public String online(HttpServletRequest request,
....
872.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1385:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1385
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	899	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
899.        public String collection(HttpServletRequest request,
....
907.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1386:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1386
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	899	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
899.        public String collection(HttpServletRequest request,
....
907.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1387:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1387
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	899	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
899.        public String collection(HttpServletRequest request,
....
907.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1388:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1388
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	899	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
899.        public String collection(HttpServletRequest request,
....
907.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1389:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1389
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	899	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
899.        public String collection(HttpServletRequest request,
....
907.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1390:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1390
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	946	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String nformation(HttpServletRequest request,

```
....
946.        public String nformation(HttpServletRequest request,
....
950.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
955.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1391:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1391
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	946	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String nformation(HttpServletRequest request,

```
....
946.        public String nformation(HttpServletRequest request,
....
950.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
955.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1392:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1392
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	946	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String nformation(HttpServletRequest request,

```
....
946.        public String nformation(HttpServletRequest request,
....
950.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
955.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1393:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1393
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	946	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String nformation(HttpServletRequest request,

```
....
946.        public String nformation(HttpServletRequest request,
....
950.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
955.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1394:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1394
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	946	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String nformation(HttpServletRequest request,

```
....
946.        public String nformation(HttpServletRequest request,
....
950.                UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
955.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1395:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1395
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	58	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1396:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1396
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1397:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1397
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1398:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1398
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1399:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1399
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1400:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1400
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	88	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1401:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1401
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1402:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1402
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1403:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1403
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1404:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1404
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1405:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1405
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	141	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1406:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1406
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	141	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1407:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1407
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	141	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1408:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1408
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	141	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1409:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1409
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	141	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1410:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1410
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	193	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1411:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1411
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	193	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1412:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1412
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	193	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1413:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1413
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	193	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1414:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1414
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	193	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1415:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1415
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	193	146
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
215.                String enterprice =
request.getParameter("enterprice");
....
218.                gasinfo.setF29e000027aa003002(enterprice);
....
231.                Pagination pagination =
enterpriseGuanZhuLanService.getPageForGasInfo(gasinfo,user.getId().toStr
ing(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public void setF29e000027aa003002(String f29e000027aa003002) {

```
....
77.   public void setF29e000027aa003002(String f29e000027aa003002) {
78.         this.f29e000027aa003002 = f29e000027aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
42.   public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
43.         return
enterpriseGuanZhuLanDao.getPageForGasInfo(gasinfo,userid,pageNo,pageSize
);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
110.        public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
....
128.              if (gasinfo.getF29e000027aa003002() != null &&
!gasinfo.getF29e000027aa003002().equals("")) {
....
130.                    sbcount.append(gasinfo.getF29e000027aa003002());
131.                    sbcount.append("%'");
....
143.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
144.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
145.              querycount.setCacheable(false);
146.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public String getF29e000027aa003002() {

```
....
73.         return f29e000027aa003002;
```

SQL Injection\路径 1416:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1416
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	244	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1417:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1417
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	244	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1418:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1418
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	244	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1419:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1419
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	244	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1420:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1420
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	244	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1421:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1421
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	295	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1422:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1422
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	295	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1423:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1423
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	295	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1424:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1424
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	295	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1425:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1425
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	295	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1426:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1426
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	295	295
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
317.              String enterprice =
request.getParameter("enterprice");
....
320.              nationaltax.setF29e000063aa003002(enterprice);
....
333.              Pagination pagination =
enterpriseGuanZhuLanService.getPageForNationalTaxInfo(nationaltax,user.g
etId().toString(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.              this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
54.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
55.         return
enterpriseGuanZhuLanDao.getPageForNationalTaxInfo(nationaltax,userid,pag
eNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
257.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
277.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
279.
      sbcount.append(nationaltax.getF29e000063aa003002());
280.                    sbcount.append("%'");
....
292.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
293.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
294.              querycount.setCacheable(false);
295.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 1427:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1427
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	346	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1428:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1428
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	346	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1429:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1429
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	346	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1430:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1430
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1431:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1431
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1432:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1432
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	346	295
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
367.                String enterprice =
request.getParameter("enterprice");
368.                String begindate = request.getParameter("begindate");
369.                String enddate = request.getParameter("enddate");
....
393.                String ntenterprice =
request.getParameter("ntenterprice");
....
396.                nationaltax.setF29e000063aa003002(ntenterprice);
....
409.                Pagination paginationNT =
enterpriseGuanZhuLanService.getPageForNationalTaxInfo(nationaltax,user.g
etId().toString(),cpn(pageNoNT),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.                this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
54.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
55.         return
enterpriseGuanZhuLanDao.getPageForNationalTaxInfo(nationaltax,userid,pag
eNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
257.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
277.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
279.
      sbcount.append(nationaltax.getF29e000063aa003002());
280.                    sbcount.append("%'");
....
292.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
293.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
294.              querycount.setCacheable(false);
295.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 1433:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1433
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	424	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1434:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1434
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	424	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1435:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1435
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	424	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1436:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1436
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	424	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1437:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1437
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	424	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1438:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1438
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	479	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1439:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1439
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	479	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1440:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1440
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	479	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1441:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1441
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	479	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1442:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1442
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	479	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1443:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1443
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	510	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1444:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1444
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	510	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1445:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1445
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	510	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1446:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1446
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	510	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1447:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1447
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	510	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1448:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1448
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	533	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1449:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1449
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	533	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1450:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1450
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	533	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1451:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1451
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	533	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1452:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1452
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	533	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1453:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1453
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	58	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1454:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1454
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1455:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1455
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1456:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1456
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1457:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1457
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanIndex(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
58.   public String guanzhulanIndex(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
66.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1458:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1458
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	88	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1459:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1459
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1460:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1460
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1461:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1461
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1462:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1462
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanWater(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
88.   public String guanzhulanWater(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
96.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1463:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1463
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	141	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1464:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1464
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	141	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1465:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1465
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	141	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1466:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1466
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	141	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1467:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1467
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	141	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanElectro(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
141.        public String guanzhulanElectro(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
149.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1468:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1468
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	193	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1469:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1469
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	193	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1470:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1470
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	193	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1471:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1471
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	193	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1472:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1472
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	193	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
201.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1473:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1473
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	193	145
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
193.        public String guanzhulanGas(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
215.                String enterprice =
request.getParameter("enterprice");
....
218.                gasinfo.setF29e000027aa003002(enterprice);
....
231.                Pagination pagination =
enterpriseGuanZhuLanServicegr.getPageForGasInfo(gasinfo,user.getId().toS
tring(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public void setF29e000027aa003002(String f29e000027aa003002) {

```
....
77.   public void setF29e000027aa003002(String f29e000027aa003002) {
78.         this.f29e000027aa003002 = f29e000027aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
52.   public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
53.         return
enterpriseGuanZhuLanDaogr.getPageForGasInfo(gasinfo,userid,pageNo,pageSi
ze);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
109.        public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
....
127.              if (gasinfo.getF29e000027aa003002() != null &&
!gasinfo.getF29e000027aa003002().equals("")) {
....
129.                    sbcount.append(gasinfo.getF29e000027aa003002());
130.                    sbcount.append("%'");
....
142.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
143.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
144.              querycount.setCacheable(false);
145.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public String getF29e000027aa003002() {

```
....
73.         return f29e000027aa003002;
```

SQL Injection\路径 1474:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1474
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	244	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1475:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1475
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	244	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1476:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1476
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	244	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1477:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1477
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	244	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1478:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1478
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	244	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanLandTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
244.        public String guanzhulanLandTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
252.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1479:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1479
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	295	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1480:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1480
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	295	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1481:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1481
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	295	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1482:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1482
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	295	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1483:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1483
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	295	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
303.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1484:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1484
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	295	294
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
295.        public String guanzhulanNationalTax(HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
317.              String enterprice =
request.getParameter("enterprice");
....
320.              nationaltax.setF29e000063aa003002(enterprice);
....
333.              Pagination pagination =
enterpriseGuanZhuLanServicegr.getPageForNationalTaxInfo(nationaltax,user
.getId().toString(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.              this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
64.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
65.         return
enterpriseGuanZhuLanDaogr.getPageForNationalTaxInfo(nationaltax,userid,p
ageNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
256.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
276.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
278.
      sbcount.append(nationaltax.getF29e000063aa003002());
279.                    sbcount.append("%'");
....
291.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
292.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
293.              querycount.setCacheable(false);
294.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 1485:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1485
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	346	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1486:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1486
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	346	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1487:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1487
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	346	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1488:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1488
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1489:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1489
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
353.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1490:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1490
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	346	294
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
346.        public String guanzhulanTaxinfo(HttpServletRequest
request,HttpServletResponse response,String selectTagNo, Integer
pageNo,Integer pageNoNT, ModelMap model) {
....
367.                String enterprice =
request.getParameter("enterprice");
368.                String begindate = request.getParameter("begindate");
369.                String enddate = request.getParameter("enddate");
....
393.                String ntenterprice =
request.getParameter("ntenterprice");
....
396.                nationaltax.setF29e000063aa003002(ntenterprice);
....
409.                Pagination paginationNT =
enterpriseGuanZhuLanServicegr.getPageForNationalTaxInfo(nationaltax,user
.getId().toString(),cpn(pageNoNT),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.                this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
64.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
65.         return
enterpriseGuanZhuLanDaogr.getPageForNationalTaxInfo(nationaltax,userid,p
ageNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
256.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
276.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
278.
      sbcount.append(nationaltax.getF29e000063aa003002());
279.                    sbcount.append("%'");
....
291.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
292.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
293.              querycount.setCacheable(false);
294.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 1491:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1491
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	424	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1492:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1492
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	424	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1493:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1493
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	424	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1494:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1494
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	424	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1495:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1495
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	424	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanPlusGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
424.        public String guanzhulanPlusGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
431.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1496:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1496
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	479	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1497:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1497
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	479	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1498:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1498
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	479	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1499:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1499
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	479	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1500:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1500
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	479	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String cancelGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
479.        public String cancelGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
486.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1501:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1501
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	510	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1502:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1502
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	510	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1503:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1503
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	510	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1504:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1504
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	510	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1505:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1505
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	510	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
510.        public String addGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
517.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1506:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1506
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	533	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1507:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1507
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	533	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1508:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1508
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	533	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1509:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1509
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	533	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1510:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1510
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	533	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String addCheckGzInfo(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
533.        public String addCheckGzInfo(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
540.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1511:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1511
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	44	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1512:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1512
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1513:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1513
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1514:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1514
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1515:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1515
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1516:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1516
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	114	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
114.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1517:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1517
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	114	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
114.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1518:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1518
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	114	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
114.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1519:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1519
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	114	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
114.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1520:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1520
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	114	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianAct.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
114.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1521:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1521
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	44	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1522:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1522
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1523:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1523
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1524:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1524
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1525:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1525
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndex(String incname,HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
44.   public String kongjianIndex(String incname,HttpServletRequest
request,HttpServletResponse response, Integer pageNo, ModelMap model) {
....
52.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1526:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1526
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	113	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
113.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1527:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1527
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	113	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
113.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1528:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1528
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	113	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
113.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1529:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1529
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	113	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
113.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1530:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1530
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	113	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseKongJianActgr.java

方法 public String kongjianIndexPost(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {

```
....
113.        public String kongjianIndexPost(String
incname,HttpServletRequest request,HttpServletResponse response,Integer
pageNoWXTS,Integer pageNoFWSC,Integer pageNo, ModelMap model) {
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1531:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1531
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1532:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1532
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1533:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1533
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1534:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1534
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1535:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1535
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongAct.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1536:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1536
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1537:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1537
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1538:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1538
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1539:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1539
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1540:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1540
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhengQiHuDongActgr.java

方法 public String zhengqihudongIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
35.   public String zhengqihudongIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
40.         String maodian = request.getParameter("maodian");
....
44.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1541:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1541
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	34	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1542:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1542
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	34	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1543:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1543
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	34	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1544:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1544
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	34	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1545:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1545
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	34	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheAct.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1546:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1546
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	34	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1547:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1547
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	34	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1548:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1548
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	34	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1549:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1549
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	34	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1550:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1550
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	34	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZhiTongCheActgr.java

方法 public String zhitongcheIndex(HttpServletRequest request,HttpServletResponse response,Integer pageNo, ModelMap model) {

```
....
34.   public String zhitongcheIndex(HttpServletRequest
request,HttpServletResponse response,Integer pageNo, ModelMap model) {
....
42.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1551:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1551
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	56	37
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java
方法	public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
56.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
61.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
62.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
63.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1552:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1552
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	56	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java
方法	public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
56.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
61.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
62.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
63.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1553:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1553
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	56	272
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
56.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
61.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
62.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
63.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1554:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1554
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	56	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
56.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
61.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
62.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
63.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
66.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1555:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1555
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	56	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
56.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
61.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
62.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
63.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
66.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1556:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1556
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	62	37
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
62.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
67.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
68.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
69.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
72.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1557:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1557
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
62.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
67.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
68.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
69.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
72.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1558:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1558
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
62.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
67.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
68.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
69.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
72.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1559:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1559
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
62.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
67.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
68.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
69.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
72.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1560:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1560
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String ZiLiaoIndex(String incname,HttpServletRequest request,HttpServletResponse response,Integer attachPageNo, Integer certPageNo, ModelMap model) {

```
....
62.   public String ZiLiaoIndex(String incname,HttpServletRequest
request,HttpServletResponse response,Integer attachPageNo, Integer
certPageNo, ModelMap model) {
....
67.         String selectTagNo = request.getParameter("selectTagNo") ==
null ? "" : request.getParameter("selectTagNo");
68.         String attachSelectTagNo =
request.getParameter("attachSelectTagNo") == null ? "" :
request.getParameter("attachSelectTagNo");
69.         String certSelectTagNo =
request.getParameter("certSelectTagNo") == null ? "" :
request.getParameter("certSelectTagNo");
....
72.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1561:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1561
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	112	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
119.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1562:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1562
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	112	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
119.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1563:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1563
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	112	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
119.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1564:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1564
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
119.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1565:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1565
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
112.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
119.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1566:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1566
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	157	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
164.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1567:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1567
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	157	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
164.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1568:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1568
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	157	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
164.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1569:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1569
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	157	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
164.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1570:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1570
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	157	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
157.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
164.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1571:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1571
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	106	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
113.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1572:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1572
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	106	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
113.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1573:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1573
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	106	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
113.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1574:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1574
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
113.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1575:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1575
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
106.        public String enterpriseStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
113.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1576:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1576
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	153	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1577:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1577
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	153	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1578:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1578
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	153	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1579:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1579
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	153	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1580:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1580
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	153	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
153.        public String enterpriseCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1581:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1581
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	364	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
367.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1582:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1582
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	364	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
367.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1583:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1583
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	364	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
367.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1584:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1584
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	364	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
367.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1585:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1585
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	364	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
364.        public String enterprisegrCancelStorePermBySxid(String
sxid,String sxzxname,String fcode,String sortcode,String
areaId,HttpServletRequest request,HttpServletResponse response, ModelMap
model){
....
367.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1586:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1586
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1001	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matter2(HttpServletRequest request,

```
....
1001.       public String matter2(HttpServletRequest request,
....
1004.               String username = request.getParameter("username");
1005.               String password = request.getParameter("password");
1006.               String sxid = request.getParameter("sxid");
....
1015.                     FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1587:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1587
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1001	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matter2(HttpServletRequest request,

```
....
1001.       public String matter2(HttpServletRequest request,
....
1004.             String username = request.getParameter("username");
1005.             String password = request.getParameter("password");
1006.             String sxid = request.getParameter("sxid");
....
1015.                   FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1588:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1588
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1001	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matter2(HttpServletRequest request,

```
....
1001.       public String matter2(HttpServletRequest request,
....
1004.             String username = request.getParameter("username");
1005.             String password = request.getParameter("password");
1006.             String sxid = request.getParameter("sxid");
....
1015.                   FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1589:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1589
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1001	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String matter2(HttpServletRequest request,

```
....
1001.       public String matter2(HttpServletRequest request,
....
1004.             String username = request.getParameter("username");
1005.             String password = request.getParameter("password");
1006.             String sxid = request.getParameter("sxid");
....
1015.                   FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1590:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1590
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1001	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String matter2(HttpServletRequest request,

```
....
1001.       public String matter2(HttpServletRequest request,
....
1004.             String username = request.getParameter("username");
1005.             String password = request.getParameter("password");
1006.             String sxid = request.getParameter("sxid");
....
1015.                   FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1591:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1591
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	105	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String memberAuthSubmit(CmsUserExt ext,HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
105.        public String memberAuthSubmit(CmsUserExt
ext,HttpServletRequest request,HttpServletResponse response, ModelMap
model) throws Exception {
....
110.              String username =  request.getParameter("username");
111.              String password1 =  request.getParameter("password1");
112.              String bankcode = request.getParameter("bankcode");
113.              String bankcardno =
request.getParameter("bankcardno");
114.              String userstatus =
request.getParameter("userstatus");
....
130.              String idType=
request.getParameter("certificatetype");
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1592:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1592
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	105	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String memberAuthSubmit(CmsUserExt ext,HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
105.        public String memberAuthSubmit(CmsUserExt
ext,HttpServletRequest request,HttpServletResponse response, ModelMap
model) throws Exception {
....
110.              String username =  request.getParameter("username");
111.              String password1 =  request.getParameter("password1");
112.              String bankcode = request.getParameter("bankcode");
113.              String bankcardno =
request.getParameter("bankcardno");
114.              String userstatus =
request.getParameter("userstatus");
....
130.              String idType=
request.getParameter("certificatetype");
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1593:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1593
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	105	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String memberAuthSubmit(CmsUserExt ext,HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
105.        public String memberAuthSubmit(CmsUserExt
ext,HttpServletRequest request,HttpServletResponse response, ModelMap
model) throws Exception {
....
110.              String username =  request.getParameter("username");
111.              String password1 =  request.getParameter("password1");
112.              String bankcode = request.getParameter("bankcode");
113.              String bankcardno =
request.getParameter("bankcardno");
114.              String userstatus =
request.getParameter("userstatus");
....
130.              String idType=
request.getParameter("certificatetype");
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1594:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1594
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	105	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String memberAuthSubmit(CmsUserExt ext,HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
105.        public String memberAuthSubmit(CmsUserExt
ext,HttpServletRequest request,HttpServletResponse response, ModelMap
model) throws Exception {
....
110.              String username =  request.getParameter("username");
111.              String password1 =  request.getParameter("password1");
112.              String bankcode = request.getParameter("bankcode");
113.              String bankcardno =
request.getParameter("bankcardno");
114.              String userstatus =
request.getParameter("userstatus");
....
130.              String idType=
request.getParameter("certificatetype");
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1595:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1595
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	105	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String memberAuthSubmit(CmsUserExt ext,HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
105.        public String memberAuthSubmit(CmsUserExt
ext,HttpServletRequest request,HttpServletResponse response, ModelMap
model) throws Exception {
....
110.              String username =  request.getParameter("username");
111.              String password1 =  request.getParameter("password1");
112.              String bankcode = request.getParameter("bankcode");
113.              String bankcardno =
request.getParameter("bankcardno");
114.              String userstatus =
request.getParameter("userstatus");
....
130.              String idType=
request.getParameter("certificatetype");
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1596:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1596
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	312	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String submit(String username, String password, String captcha,

```
....
312.                    HttpServletRequest request, HttpServletResponse
response,
....
450.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1597:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1597
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	312	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String submit(String username, String password, String captcha,

```
....
312.                    HttpServletRequest request, HttpServletResponse
response,
....
450.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1598:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1598
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	312	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String submit(String username, String password, String captcha,

```
....
312.                    HttpServletRequest request, HttpServletResponse
response,
....
450.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1599:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1599
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	312	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String submit(String username, String password, String captcha,

```
....
312.                    HttpServletRequest request, HttpServletResponse
response,
....
450.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1600:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1600
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	312	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String submit(String username, String password, String captcha,

```
....
312.                    HttpServletRequest request, HttpServletResponse
response,
....
450.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1601:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1601
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	145	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1602:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1602
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	145	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1603:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1603
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	145	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1604:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1604
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java
方法	public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1605:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1605
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1606:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1606
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	145	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1607:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1607
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	145	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1608:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1608
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	145	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1609:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1609
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1610:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1610
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java
方法	public String submit(String username, String password, String captcha,

```
....
145.                    HttpServletRequest request, HttpServletResponse
response,
....
206.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1611:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1611
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	241	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userResult(String username, String password,String tokenId,

```
....
241.                    String captcha_find, HttpServletRequest request,
....
244.                captcha_find = request.getParameter("captcha_find");
....
251.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1612:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1612
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	241	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userResult(String username, String password,String tokenId,

```
....
241.                    String captcha_find, HttpServletRequest request,
....
244.              captcha_find = request.getParameter("captcha_find");
....
251.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1613:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1613
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	241	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userResult(String username, String password,String tokenId,

```
....
241.                    String captcha_find, HttpServletRequest request,
....
244.              captcha_find = request.getParameter("captcha_find");
....
251.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1614:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1614
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	241	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String new_userResult(String username, String password,String tokenId,

```
....
241.                    String captcha_find, HttpServletRequest request,
....
244.              captcha_find = request.getParameter("captcha_find");
....
251.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1615:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1615
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	241	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userResult(String username, String password,String tokenId,

```
....
241.                    String captcha_find, HttpServletRequest request,
....
244.              captcha_find = request.getParameter("captcha_find");
....
251.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1616:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1616
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	275	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userAdd(String tokenId, HttpServletRequest request,

```
....
275.        public String new_userAdd(String tokenId, HttpServletRequest
request,
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1617:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1617
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	275	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userAdd(String tokenId, HttpServletRequest request,

```
....
275.        public String new_userAdd(String tokenId, HttpServletRequest
request,
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1618:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1618
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	275	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userAdd(String tokenId, HttpServletRequest request,

```
....
275.        public String new_userAdd(String tokenId, HttpServletRequest
request,
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1619:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1619
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	275	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String new_userAdd(String tokenId, HttpServletRequest request,

```
....
275.        public String new_userAdd(String tokenId, HttpServletRequest
request,
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1620:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1620
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	275	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String new_userAdd(String tokenId, HttpServletRequest request,

```
....
275.        public String new_userAdd(String tokenId, HttpServletRequest
request,
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1621:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1621
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	124	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java
方法	public String submit(String username, String email, String password,

```
....
124.                    HttpServletRequest request, HttpServletResponse
response,
....
138.              String userpid = request.getParameter("userpid");
139.              String certificatetype =
request.getParameter("certificatetype");
140.              String usertype = request.getParameter("usertype");
141.              String userphone = request.getParameter("userphone");
142.              String bankcode = request.getParameter("bankcode");
143.              String bankcardno =
request.getParameter("bankcardno");
144.              String agephone = request.getParameter("agephone");
145.              String ageindicia =
request.getParameter("ageindicia");
146.              String ageaddr = request.getParameter("ageaddr");
....
245.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1622:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1622
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	124	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String submit(String username, String email, String password,

```
....
124.                    HttpServletRequest request, HttpServletResponse
response,
....
138.              String userpid = request.getParameter("userpid");
139.              String certificatetype =
request.getParameter("certificatetype");
140.              String usertype = request.getParameter("usertype");
141.              String userphone = request.getParameter("userphone");
142.              String bankcode = request.getParameter("bankcode");
143.              String bankcardno =
request.getParameter("bankcardno");
144.              String agephone = request.getParameter("agephone");
145.              String ageindicia =
request.getParameter("ageindicia");
146.              String ageaddr = request.getParameter("ageaddr");
....
245.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1623:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1623
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	124	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String submit(String username, String email, String password,

```
....
124.                    HttpServletRequest request, HttpServletResponse
response,
....
138.              String userpid = request.getParameter("userpid");
139.              String certificatetype =
request.getParameter("certificatetype");
140.              String usertype = request.getParameter("usertype");
141.              String userphone = request.getParameter("userphone");
142.              String bankcode = request.getParameter("bankcode");
143.              String bankcardno =
request.getParameter("bankcardno");
144.              String agephone = request.getParameter("agephone");
145.              String ageindicia =
request.getParameter("ageindicia");
146.              String ageaddr = request.getParameter("ageaddr");
....
245.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1624:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1624
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	124	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String submit(String username, String email, String password,

```
....
124.                    HttpServletRequest request, HttpServletResponse
response,
....
138.              String userpid = request.getParameter("userpid");
139.              String certificatetype =
request.getParameter("certificatetype");
140.              String usertype = request.getParameter("usertype");
141.              String userphone = request.getParameter("userphone");
142.              String bankcode = request.getParameter("bankcode");
143.              String bankcardno =
request.getParameter("bankcardno");
144.              String agephone = request.getParameter("agephone");
145.              String ageindicia =
request.getParameter("ageindicia");
146.              String ageaddr = request.getParameter("ageaddr");
....
245.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1625:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1625
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	124	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String submit(String username, String email, String password,

```
....
124.                    HttpServletRequest request, HttpServletResponse
response,
....
138.                String userpid = request.getParameter("userpid");
139.                String certificatetype =
request.getParameter("certificatetype");
140.                String usertype = request.getParameter("usertype");
141.                String userphone = request.getParameter("userphone");
142.                String bankcode = request.getParameter("bankcode");
143.                String bankcardno =
request.getParameter("bankcardno");
144.                String agephone = request.getParameter("agephone");
145.                String ageindicia =
request.getParameter("ageindicia");
146.                String ageaddr = request.getParameter("ageaddr");
....
245.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1626:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1626
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	380	37
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java
方法	public String caRegisterSubmit(String username, String email,

```
....
380.                    String nextUrl, HttpServletRequest request,
....
383.              String registercaptcha =
request.getParameter("registercaptcha");
....
392.              properties.load(new
FileInputStream(request.getRealPath("WEB-INF")
....
398.              String clientCert = request.getParameter("UserCert");
399.              String UserSignedData =
request.getParameter("UserSignedData");
400.              String ContainerName =
request.getParameter("ContainerName");
....
412.              String usertype = request.getParameter("usertype");
....
510.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1627:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1627
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	380	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterSubmit(String username, String email,

```
....
380.                    String nextUrl, HttpServletRequest request,
....
383.              String registercaptcha =
request.getParameter("registercaptcha");
....
392.              properties.load(new
FileInputStream(request.getRealPath("WEB-INF")
....
398.              String clientCert = request.getParameter("UserCert");
399.              String UserSignedData =
request.getParameter("UserSignedData");
400.              String ContainerName =
request.getParameter("ContainerName");
....
412.              String usertype = request.getParameter("usertype");
....
510.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1628:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1628
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	380	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterSubmit(String username, String email,

```
....
380.                    String nextUrl, HttpServletRequest request,
....
383.              String registercaptcha =
request.getParameter("registercaptcha");
....
392.              properties.load(new
FileInputStream(request.getRealPath("WEB-INF")
....
398.              String clientCert = request.getParameter("UserCert");
399.              String UserSignedData =
request.getParameter("UserSignedData");
400.              String ContainerName =
request.getParameter("ContainerName");
....
412.              String usertype = request.getParameter("usertype");
....
510.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1629:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1629
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	380	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterSubmit(String username, String email,

```
....
380.                    String nextUrl, HttpServletRequest request,
....
383.              String registercaptcha =
request.getParameter("registercaptcha");
....
392.              properties.load(new
FileInputStream(request.getRealPath("WEB-INF")
....
398.              String clientCert = request.getParameter("UserCert");
399.              String UserSignedData =
request.getParameter("UserSignedData");
400.              String ContainerName =
request.getParameter("ContainerName");
....
412.              String usertype = request.getParameter("usertype");
....
510.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1630:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1630
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	380	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterSubmit(String username, String email,

```
....
380.                    String nextUrl, HttpServletRequest request,
....
383.                String registercaptcha =
request.getParameter("registercaptcha");
....
392.                properties.load(new
FileInputStream(request.getRealPath("WEB-INF")
....
398.                String clientCert = request.getParameter("UserCert");
399.                String UserSignedData =
request.getParameter("UserSignedData");
400.                String ContainerName =
request.getParameter("ContainerName");
....
412.                String usertype = request.getParameter("usertype");
....
510.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1631:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1631
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	557	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String active(String username, String key,

```
....
557.                    HttpServletRequest request, HttpServletResponse
response,
....
562.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1632:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1632
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	557	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String active(String username, String key,

```
....
557.                    HttpServletRequest request, HttpServletResponse
response,
....
562.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1633:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1633
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	557	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String active(String username, String key,

```
....
557.                    HttpServletRequest request, HttpServletResponse
response,
....
562.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1634:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1634
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	557	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String active(String username, String key,

```
....
557.                    HttpServletRequest request, HttpServletResponse
response,
....
562.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1635:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1635
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	557	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String active(String username, String key,

```
....
557.                    HttpServletRequest request, HttpServletResponse
response,
....
562.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1636:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1636
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	113	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1637:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1637
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	113	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1638:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1638
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	113	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1639:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1639
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	113	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1640:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1640
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	113	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1641:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1641
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	626	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String indexForWeblogic(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
626.        public String indexForWeblogic(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
627.                return index(request,response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1642:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1642
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	626	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String indexForWeblogic(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
626.        public String indexForWeblogic(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
627.              return index(request,response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1643:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1643
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	626	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String indexForWeblogic(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
626.        public String indexForWeblogic(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
627.                return index(request,response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1644:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1644
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	626	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String indexForWeblogic(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
626.        public String indexForWeblogic(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
627.                return index(request,response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1645:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1645
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	626	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String indexForWeblogic(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
626.        public String indexForWeblogic(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
627.              return index(request,response, model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index(HttpServletRequest request,HttpServletResponse response, ModelMap model) {

```
....
113.        public String index(HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
116.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1646:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1646
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	459	37
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String caLogin(String username, String password, String captcha,

```
....
459.                    HttpServletRequest request, HttpServletResponse
response,
....
465.              properties.load(new
FileInputStream(request.getRealPath("WEB-
INF").concat("/config/webappName.properties")));
....
469.              String clientCert = request.getParameter("UserCert");
470.              String UserSignedData =
request.getParameter("UserSignedData");
471.              String ContainerName =
request.getParameter("ContainerName");
....
541.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1647:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1647
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	459	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String caLogin(String username, String password, String captcha,

```
....
459.                     HttpServletRequest request, HttpServletResponse
response,
....
465.               properties.load(new
FileInputStream(request.getRealPath("WEB-
INF").concat("/config/webappName.properties")));
....
469.               String clientCert = request.getParameter("UserCert");
470.               String UserSignedData =
request.getParameter("UserSignedData");
471.               String ContainerName =
request.getParameter("ContainerName");
....
541.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1648:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1648
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	459	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String caLogin(String username, String password, String captcha,

```
....
459.                    HttpServletRequest request, HttpServletResponse
response,
....
465.                properties.load(new
FileInputStream(request.getRealPath("WEB-
INF").concat("/config/webappName.properties")));
....
469.                String clientCert = request.getParameter("UserCert");
470.                String UserSignedData =
request.getParameter("UserSignedData");
471.                String ContainerName =
request.getParameter("ContainerName");
....
541.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1649:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1649
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	459	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String caLogin(String username, String password, String captcha,

```
....
459.                    HttpServletRequest request, HttpServletResponse
response,
....
465.                properties.load(new
FileInputStream(request.getRealPath("WEB-
INF").concat("/config/webappName.properties")));
....
469.                String clientCert = request.getParameter("UserCert");
470.                String UserSignedData =
request.getParameter("UserSignedData");
471.                String ContainerName =
request.getParameter("ContainerName");
....
541.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1650:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1650
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	459	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String caLogin(String username, String password, String captcha,

```
....
459.                    HttpServletRequest request, HttpServletResponse
response,
....
465.                properties.load(new
FileInputStream(request.getRealPath("WEB-
INF").concat("/config/webappName.properties")));
....
469.                String clientCert = request.getParameter("UserCert");
470.                String UserSignedData =
request.getParameter("UserSignedData");
471.                String ContainerName =
request.getParameter("ContainerName");
....
541.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1651:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1651
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	335	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterInput(HttpServletRequest request,

```
....
335.        public String caRegisterInput(HttpServletRequest request,
....
346.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1652:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1652
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	335	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterInput(HttpServletRequest request,

```
....
335.        public String caRegisterInput(HttpServletRequest request,
....
346.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1653:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1653
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	335	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterInput(HttpServletRequest request,

```
....
335.        public String caRegisterInput(HttpServletRequest request,
....
346.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1654:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1654
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	335	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterInput(HttpServletRequest request,

```
....
335.        public String caRegisterInput(HttpServletRequest request,
....
346.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1655:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1655
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	335	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String caRegisterInput(HttpServletRequest request,

```
....
335.        public String caRegisterInput(HttpServletRequest request,
....
346.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1656:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1656
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	132	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String submit(String username, String password, String captcha, String processUrl, String returnUrl,

```
....
132.                String message, HttpServletRequest request,
HttpServletResponse response, ModelMap model)
....
190.            FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1657:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1657
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	132	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String submit(String username, String password, String captcha, String processUrl, String returnUrl,

```
....
132.              String message, HttpServletRequest request,
HttpServletResponse response, ModelMap model)
....
190.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1658:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1658
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	132	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String submit(String username, String password, String captcha, String processUrl, String returnUrl,

```
....
132.              String message, HttpServletRequest request,
HttpServletResponse response, ModelMap model)
....
190.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1659:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1659
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	132	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String submit(String username, String password, String captcha, String processUrl, String returnUrl,

```
....
132.              String message, HttpServletRequest request,
HttpServletResponse response, ModelMap model)
....
190.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1660:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1660
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	132	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String submit(String username, String password, String captcha, String processUrl, String returnUrl,

```
....
132.              String message, HttpServletRequest request,
HttpServletResponse response, ModelMap model)
....
190.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1661:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1661
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	152	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
152.                    String nextUrl, HttpServletRequest request,
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1662:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1662
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	152	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
152.                    String nextUrl, HttpServletRequest request,
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1663:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1663
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	152	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
152.                    String nextUrl, HttpServletRequest request,
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1664:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1664
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	152	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
152.                    String nextUrl, HttpServletRequest request,
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1665:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1665
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	152	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
152.                    String nextUrl, HttpServletRequest request,
....
160.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1666:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1666
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	217	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_send(CmsMessage message, String username,

```
....
217.                    String captcha, String nextUrl,
HttpServletRequest request,
....
225.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1667:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1667
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	217	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_send(CmsMessage message, String username,

```
....
217.                    String captcha, String nextUrl,
HttpServletRequest request,
....
225.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1668:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1668
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	217	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_send(CmsMessage message, String username,

```
....
217.                    String captcha, String nextUrl,
HttpServletRequest request,
....
225.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1669:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1669
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	217	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_send(CmsMessage message, String username,

```
....
217.                    String captcha, String nextUrl,
HttpServletRequest request,
....
225.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1670:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1670
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	217	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_send(CmsMessage message, String username,

```
....
217.                    String captcha, String nextUrl,
HttpServletRequest request,
....
225.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1671:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1671
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	256	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_save(CmsMessage message, String username,

```
....
256.                    String captcha, String nextUrl,
HttpServletRequest request,
....
264.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1672:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1672
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	256	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_save(CmsMessage message, String username,

```
....
256.                    String captcha, String nextUrl,
HttpServletRequest request,
....
264.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1673:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1673
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	256	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_save(CmsMessage message, String username,

```
....
256.                    String captcha, String nextUrl,
HttpServletRequest request,
....
264.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1674:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1674
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	256	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_save(CmsMessage message, String username,

```
....
256.                    String captcha, String nextUrl,
HttpServletRequest request,
....
264.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1675:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1675
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	256	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_save(CmsMessage message, String username,

```
....
256.                    String captcha, String nextUrl,
HttpServletRequest request,
....
264.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1676:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1676
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	294	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_tosend(Integer id, String nextUrl, String captcha,

```
....
294.                    HttpServletRequest request, HttpServletResponse
response,
....
302.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1677:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1677
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	294	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_tosend(Integer id, String nextUrl, String captcha,

```
....
294.                    HttpServletRequest request, HttpServletResponse
response,
....
302.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1678:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1678
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	294	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_tosend(Integer id, String nextUrl, String captcha,

```
....
294.                    HttpServletRequest request, HttpServletResponse
response,
....
302.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1679:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1679
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	294	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_tosend(Integer id, String nextUrl, String captcha,

```
....
294.                    HttpServletRequest request, HttpServletResponse
response,
....
302.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1680:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1680
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	294	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_tosend(Integer id, String nextUrl, String captcha,

```
....
294.                    HttpServletRequest request, HttpServletResponse
response,
....
302.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1681:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1681
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	359	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_update(CmsMessage message, String nextUrl,

```
....
359.                    String captcha, HttpServletRequest request,
....
367.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1682:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1682
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	359	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_update(CmsMessage message, String nextUrl,

```
....
359.                    String captcha, HttpServletRequest request,
....
367.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1683:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1683
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	359	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_update(CmsMessage message, String nextUrl,

```
....
359.                    String captcha, HttpServletRequest request,
....
367.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1684:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1684
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	359	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_update(CmsMessage message, String nextUrl,

```
....
359.                    String captcha, HttpServletRequest request,
....
367.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1685:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1685
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	359	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_update(CmsMessage message, String nextUrl,

```
....
359.                    String captcha, HttpServletRequest request,
....
367.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1686:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1686
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	488	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
488.        public String index4(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
490.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1687:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1687
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	488	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
488.        public String index4(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
490.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1688:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1688
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	488	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
488.        public String index4(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
490.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1689:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1689
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	488	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index4(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
488.        public String index4(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
490.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1690:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1690
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	488	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index4(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
488.        public String index4(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
490.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1691:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1691
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	530	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Post(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
530.        public String index4Post(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
532.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1692:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1692
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	530	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Post(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
530.        public String index4Post(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
532.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1693:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1693
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	530	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Post(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
530.        public String index4Post(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
532.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1694:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1694
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	530	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index4Post(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
530.        public String index4Post(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
532.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1695:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1695
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	530	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index4Post(Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
530.        public String index4Post(Integer pageNo,HttpServletRequest
request, ModelMap model) {
....
532.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1696:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1696
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	138	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
141.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1697:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1697

结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	138	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
141.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1698:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1698
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	138	272
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
141.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.                if(areaId != null && !areaId.equals("")){
....
119.                        request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1699:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1699
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
141.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1700:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1700
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
141.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1701:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1701
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	182	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
185.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1702:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1702
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	182	241
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
185.              areaId = chickAreaId(areaId,request);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1703:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1703
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	182	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
185.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1704:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1704
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
185.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.                if(areaId != null && !areaId.equals("")){
....
119.                        request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1705:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1705
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	247
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
185.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
103.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
105.              if(areaId != null && !areaId.equals("")){
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1706:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1706
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	311	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String list(String deptId, String permtype,

```
....
311.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
313.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
314.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1707:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1707
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	311	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String list(String deptId, String permtype,

```
....
311.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
313.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
314.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1708:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1708
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	311	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String list(String deptId, String permtype,

```
....
311.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
313.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
314.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1709:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1709
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	311	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String list(String deptId, String permtype,

```
....
311.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
313.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
314.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1710:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1710
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	311	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String list(String deptId, String permtype,

```
....
311.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
313.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
314.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1711:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1711
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	389	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listsxinfo(String deptId, String permtype,

```
....
389.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
391.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
392.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1712:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1712
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	389	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listsxinfo(String deptId, String permtype,

```
....
389.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
391.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
392.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1713:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1713
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	389	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listsxinfo(String deptId, String permtype,

```
....
389.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
391.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
392.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1714:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1714
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	389	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String listsxinfo(String deptId, String permtype,

```
....
389.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
391.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
392.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1715:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1715
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	389	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listsxinfo(String deptId, String permtype,

```
....
389.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
391.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
392.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1716:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1716
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	821	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermByName(String selname,

```
....
821.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
823.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1717:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1717
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	821	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermByName(String selname,

```
....
821.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1718:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1718
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	821	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermByName(String selname,

```
....
821.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1719:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1719
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	821	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String listPermByName(String selname,

```
....
821.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1720:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1720
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	821	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermByName(String selname,

```
....
821.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1721:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1721
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	842	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermBySort(String sortcode,

```
....
842.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
844.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1722:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1722
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	842	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermBySort(String sortcode,

```
....
842.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
844.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1723:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1723
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	842	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermBySort(String sortcode,

```
....
842.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
844.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1724:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1724
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	842	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String listPermBySort(String sortcode,

```
....
842.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
844.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1725:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1725
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	842	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String listPermBySort(String sortcode,

```
....
842.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
844.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1726:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1726
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	999	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem(Integer pageNo,HttpServletRequest request,

```
....
999.        public String regionpermissionitem(Integer
pageNo,HttpServletRequest request,
....
1002.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1727:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1727
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	999	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem(Integer pageNo,HttpServletRequest request,

```
....
999.        public String regionpermissionitem(Integer
pageNo,HttpServletRequest request,
....
1002.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1728:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1728
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	999	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem(Integer pageNo,HttpServletRequest request,

```
....
999.        public String regionpermissionitem(Integer
pageNo,HttpServletRequest request,
....
1002.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1729:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1729
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	999	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String regionpermissionitem(Integer pageNo,HttpServletRequest request,

```
....
999.        public String regionpermissionitem(Integer
pageNo,HttpServletRequest request,
....
1002.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1730:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1730
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	999	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem(Integer pageNo,HttpServletRequest request,

```
....
999.        public String regionpermissionitem(Integer
pageNo,HttpServletRequest request,
....
1002.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1731:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1731
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1030	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(Integer pageNo,HttpServletRequest request,

```
....
1030.       public String regionpermissionitem1(Integer
pageNo,HttpServletRequest request,
....
1033.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1732:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1732
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1030	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(Integer pageNo,HttpServletRequest request,

```
....
1030.       public String regionpermissionitem1(Integer
pageNo,HttpServletRequest request,
....
1033.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1733:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1733
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1030	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(Integer pageNo,HttpServletRequest request,

```
....
1030.       public String regionpermissionitem1(Integer
pageNo,HttpServletRequest request,
....
1033.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1734:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1734
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1030	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String regionpermissionitem1(Integer pageNo,HttpServletRequest request,

```
....
1030.       public String regionpermissionitem1(Integer
pageNo,HttpServletRequest request,
....
1033.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1735:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1735
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1030	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(Integer pageNo,HttpServletRequest request,

```
....
1030.       public String regionpermissionitem1(Integer
pageNo,HttpServletRequest request,
....
1033.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1736:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1736
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1063	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(String sortcode,Integer pageNo,HttpServletRequest request,

```
....
1063.       public String regionpermissionitem1(String sortcode,Integer
pageNo,HttpServletRequest request,
....
1066.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1737:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1737
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1063	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(String sortcode,Integer pageNo,HttpServletRequest request,

```
....
1063.       public String regionpermissionitem1(String sortcode,Integer
pageNo,HttpServletRequest request,
....
1066.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1738:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1738
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1063	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String regionpermissionitem1(String sortcode,Integer pageNo,HttpServletRequest request,

```
....
1063.       public String regionpermissionitem1(String sortcode,Integer
pageNo,HttpServletRequest request,
....
1066.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1739:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1739
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1063	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String regionpermissionitem1(String sortcode,Integer pageNo,HttpServletRequest request,

```
....
1063.       public String regionpermissionitem1(String sortcode,Integer
pageNo,HttpServletRequest request,
....
1066.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1740:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1740
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1063	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String regionpermissionitem1(String sortcode,Integer pageNo,HttpServletRequest request,

```
....
1063.       public String regionpermissionitem1(String sortcode,Integer
pageNo,HttpServletRequest request,
....
1066.               FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1741:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1741
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	151	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
155.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
129.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
131.              if(areaId != null && !areaId.equals("")){
....
145.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1742:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1742

结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
155.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
129.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
131.                if(areaId != null && !areaId.equals("")){
....
145.                        request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1743:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1743
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	272
对象	areaId	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
155.              areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
129.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
131.              if(areaId != null && !areaId.equals("")){
....
145.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1744:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1744
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
155.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
129.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
131.              if(areaId != null && !areaId.equals("")){
....
145.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1745:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1745
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
155.                areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
129.        public String chickAreaId(String areaId,HttpServletRequest
request){
....
131.                if(areaId != null && !areaId.equals("")){
....
145.                        request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1746:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1746
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	307	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String listPermBySort(String sortcode,

```
....
307.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
309.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1747:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1747
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	307	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String listPermBySort(String sortcode,

```
....
307.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
309.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1748:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1748
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	307	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String listPermBySort(String sortcode,

```
....
307.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
309.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1749:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1749
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	307	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String listPermBySort(String sortcode,

```
....
307.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
309.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1750:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1750
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	307	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String listPermBySort(String sortcode,

```
....
307.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
309.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1751:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1751
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	682	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
689.          areaId = chickAreaId(areaId, request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String chickAreaId(String areaId, HttpServletRequest request) {

```
....
650.      public String chickAreaId(String areaId, HttpServletRequest
request) {
....
652.          if (areaId != null && !areaId.equals("")) {
....
666.              request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1752:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1752

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	682	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
689.          areaId = chickAreaId(areaId, request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String chickAreaId(String areaId, HttpServletRequest request) {

```
....
650.      public String chickAreaId(String areaId, HttpServletRequest
request) {
....
652.          if (areaId != null && !areaId.equals("")) {
....
666.              request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1753:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1753
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	682	272
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
689.          areaId = chickAreaId(areaId, request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String chickAreaId(String areaId, HttpServletRequest request) {

```
....
650.      public String chickAreaId(String areaId, HttpServletRequest
request) {
....
652.          if (areaId != null && !areaId.equals("")) {
....
666.              request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1754:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1754
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	682	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
689.          areaId = chickAreaId(areaId, request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String chickAreaId(String areaId, HttpServletRequest request) {

```
....
650.      public String chickAreaId(String areaId, HttpServletRequest
request) {
....
652.          if (areaId != null && !areaId.equals("")) {
....
666.              request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1755:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1755
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	682	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
689.          areaId = chickAreaId(areaId, request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String chickAreaId(String areaId, HttpServletRequest request) {

```
....
650.      public String chickAreaId(String areaId, HttpServletRequest
request) {
....
652.          if (areaId != null && !areaId.equals("")) {
....
666.              request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1756:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1756
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	36	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
70.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
72.         if(areaId != null && !areaId.equals("")){
....
86.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1757:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1757
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	36	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
70.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
72.         if(areaId != null && !areaId.equals("")){
....
86.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1758:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1758
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	36	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
70.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
72.         if(areaId != null && !areaId.equals("")){
....
86.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1759:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1759
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
70.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
72.         if(areaId != null && !areaId.equals("")){
....
86.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1760:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1760
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	247
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
70.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
72.         if(areaId != null && !areaId.equals("")){
....
86.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1761:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1761
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1762:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1762

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1763:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1763
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	areaId	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1764:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1764
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1765:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1765
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1766:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1766
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	45	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
48.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
80.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
82.         if(areaId != null && !areaId.equals("")){
....
96.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1767:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1767
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	45	241
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
48.         areaId = chickAreaId(areaId,request);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String chickAreaId(String areaId,HttpServletRequest request){

```
....
80.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
82.         if(areaId != null && !areaId.equals("")){
....
96.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1768:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1768
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	45	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
48.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
80.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
82.         if(areaId != null && !areaId.equals("")){
....
96.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1769:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1769
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	45	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
48.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
80.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
82.         if(areaId != null && !areaId.equals("")){
....
96.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1770:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1770
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	45	247
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
48.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
80.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
82.         if(areaId != null && !areaId.equals("")){
....
96.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1771:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1771
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	41	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
44.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
75.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
77.         if(areaId != null && !areaId.equals("")){
....
91.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1772:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1772

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
44.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
75.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
77.         if(areaId != null && !areaId.equals("")){
....
91.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1773:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1773
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	272
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
44.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
75.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
77.         if(areaId != null && !areaId.equals("")){
....
91.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1774:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1774
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
44.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
75.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
77.         if(areaId != null && !areaId.equals("")){
....
91.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1775:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1775
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
44.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
75.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
77.         if(areaId != null && !areaId.equals("")){
....
91.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1776:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1776
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1777:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1777
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1778:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1778
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1779:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1779
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1780:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1780
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1781:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1781
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1782:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1782

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1783:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1783
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	areaId	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1784:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1784
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1785:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1785
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
38.         areaId = chickAreaId(areaId,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
69.   public String chickAreaId(String areaId,HttpServletRequest
request){
....
71.         if(areaId != null && !areaId.equals("")){
....
85.               request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1786:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1786
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	325	37
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1787:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1787
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	325	241
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1788:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1788
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	325	272
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1789:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1789
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	325	218
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1790:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1790
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	325	247
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1791:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1791
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	38	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String ad(Integer id, HttpServletRequest request,

```
....
38.   public String ad(Integer id, HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1792:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1792
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	38	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String ad(Integer id, HttpServletRequest request,

```
....
38.   public String ad(Integer id, HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1793:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1793
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	38	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String ad(Integer id, HttpServletRequest request,

```
....
38.   public String ad(Integer id, HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1794:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1794
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	38	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java
方法	public String ad(Integer id, HttpServletRequest request,

```
....
38.   public String ad(Integer id, HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1795:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1795
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	38	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String ad(Integer id, HttpServletRequest request,

```
....
38.   public String ad(Integer id, HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1796:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1796
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	46	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String page(Integer contentId, Integer pageNo,

```
....
46.                 HttpServletRequest request, HttpServletResponse
response,
....
59.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1797:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1797
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	46	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String page(Integer contentId, Integer pageNo,

```
....
46.                 HttpServletRequest request, HttpServletResponse
response,
....
59.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1798:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1798
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	46	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String page(Integer contentId, Integer pageNo,

```
....
46.                HttpServletRequest request, HttpServletResponse
response,
....
59.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.         public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1799:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1799
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java
方法	public String page(Integer contentId, Integer pageNo,

```
....
46.                HttpServletRequest request, HttpServletResponse
response,
....
59.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.         public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.    public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.          return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 1800:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1800
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String page(Integer contentId, Integer pageNo,

```
....
46.               HttpServletRequest request, HttpServletResponse
response,
....
59.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1801:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1801
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	634	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String dynamic(HttpServletRequest request,

```
....
634.        public String dynamic(HttpServletRequest request,
....
657.                                return content(id, pageNo, params,
info, request, response,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String content(Integer id, int pageNo, String[] params,

```
....
688.                    PageInfo info, HttpServletRequest request,
....
716.                          return FrontUtils.showMessage(request,
model, GROUP_FORBIDDEN,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1802:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1802
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	634	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String dynamic(HttpServletRequest request,

```
....
634.        public String dynamic(HttpServletRequest request,
....
657.                                  return content(id, pageNo, params,
info, request, response,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String content(Integer id, int pageNo, String[] params,

```
....
688.                    PageInfo info, HttpServletRequest request,
....
716.                            return FrontUtils.showMessage(request,
model, GROUP_FORBIDDEN,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 1803:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1803
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	634	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String dynamic(HttpServletRequest request,

```
....
634.        public String dynamic(HttpServletRequest request,
....
657.                                    return content(id, pageNo, params,
info, request, response,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String content(Integer id, int pageNo, String[] params,

```
....
688.                    PageInfo info, HttpServletRequest request,
....
716.                            return FrontUtils.showMessage(request,
model, GROUP_FORBIDDEN,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1804:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1804
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	634	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String dynamic(HttpServletRequest request,

```
....
634.        public String dynamic(HttpServletRequest request,
....
657.                                    return content(id, pageNo, params,
info, request, response,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String content(Integer id, int pageNo, String[] params,

```
....
688.                    PageInfo info, HttpServletRequest request,
....
716.                           return FrontUtils.showMessage(request,
model, GROUP_FORBIDDEN,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1805:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1805
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	634	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String dynamic(HttpServletRequest request,

```
....
634.        public String dynamic(HttpServletRequest request,
....
657.                                    return content(id, pageNo, params,
info, request, response,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String content(Integer id, int pageNo, String[] params,

```
....
688.                    PageInfo info, HttpServletRequest request,
....
716.                            return FrontUtils.showMessage(request,
model, GROUP_FORBIDDEN,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1806:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1806
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	48	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java
方法	public String advice_add(String bsnum, String result,

```
....
48.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
55.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1807:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1807
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String advice_add(String bsnum, String result,

```
....
48.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
55.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1808:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1808
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String advice_add(String bsnum, String result,

```
....
48.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
55.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1809:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1809
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String advice_add(String bsnum, String result,

```
....
48.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
55.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1810:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1810
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String advice_add(String bsnum, String result,

```
....
48.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
55.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1811:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1811
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	123	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
123.        public String opinionRecord_list(String title,Integer
pageNo, HttpServletRequest request, ModelMap model) {
....
135.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1812:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1812
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	123	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
123.        public String opinionRecord_list(String title,Integer
pageNo, HttpServletRequest request, ModelMap model) {
....
135.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1813:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1813
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	123	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
123.        public String opinionRecord_list(String title,Integer
pageNo, HttpServletRequest request, ModelMap model) {
....
135.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1814:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1814
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	123	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
123.        public String opinionRecord_list(String title,Integer
pageNo, HttpServletRequest request, ModelMap model) {
....
135.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1815:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1815
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	123	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
123.        public String opinionRecord_list(String title,Integer
pageNo, HttpServletRequest request, ModelMap model) {
....
135.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1816:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1816
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	151	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_detail(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
151.        public String opinionRecord_detail(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
161.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1817:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1817
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_detail(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
151.        public String opinionRecord_detail(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
161.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1818:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1818
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_detail(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
151.        public String opinionRecord_detail(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
161.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1819:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1819
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_detail(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
151.        public String opinionRecord_detail(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
161.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1820:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1820
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord_detail(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
151.        public String opinionRecord_detail(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
161.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1821:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1821
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	151	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
166.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1822:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1822
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
166.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1823:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1823
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
166.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1824:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1824
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
166.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1825:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1825
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbdeptlist(String areaId,String sxid, HttpServletRequest request,

```
....
151.        public String wssbdeptlist(String areaId,String sxid,
HttpServletRequest request,
....
166.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1826:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1826
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	237	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtml(String sxid, HttpServletRequest request,

```
....
237.        public String matterhtml(String sxid, HttpServletRequest
request,
....
246.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1827:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1827
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	237	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtml(String sxid, HttpServletRequest request,

```
....
237.        public String matterhtml(String sxid, HttpServletRequest
request,
....
246.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1828:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1828
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	237	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtml(String sxid, HttpServletRequest request,

```
....
237.        public String matterhtml(String sxid, HttpServletRequest
request,
....
246.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1829:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1829
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	237	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtml(String sxid, HttpServletRequest request,

```
....
237.        public String matterhtml(String sxid, HttpServletRequest
request,
....
246.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1830:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1830
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	237	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtml(String sxid, HttpServletRequest request,

```
....
237.        public String matterhtml(String sxid, HttpServletRequest
request,
....
246.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1831:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1831
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	933	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
941.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1832:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1832
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	933	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
941.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1833:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1833
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	933	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
941.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1834:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1834
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	933	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
941.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1835:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1835
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	933	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
941.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1836:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1836
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	59	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String list(String queryTitle, String deptId,

```
....
59.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
71.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1837:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1837
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String list(String queryTitle, String deptId,

```
....
59.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
71.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1838:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1838
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String list(String queryTitle, String deptId,

```
....
59.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
71.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1839:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1839
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String list(String queryTitle, String deptId,

```
....
59.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
71.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1840:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1840
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String list(String queryTitle, String deptId,

```
....
59.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
71.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1841:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1841
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	97	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String add(HttpServletRequest request, ModelMap model,String sxid) {

```
....
97.   public String add(HttpServletRequest request, ModelMap
model,String sxid) {
....
106.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1842:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1842
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	97	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String add(HttpServletRequest request, ModelMap model,String sxid) {

```
....
97.   public String add(HttpServletRequest request, ModelMap
model,String sxid) {
....
106.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1843:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1843
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	97	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String add(HttpServletRequest request, ModelMap model,String sxid) {

```
....
97.   public String add(HttpServletRequest request, ModelMap
model,String sxid) {
....
106.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1844:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1844
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	97	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String add(HttpServletRequest request, ModelMap model,String sxid) {

```
....
97.   public String add(HttpServletRequest request, ModelMap
model,String sxid) {
....
106.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1845:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1845
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	97	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String add(HttpServletRequest request, ModelMap model,String sxid) {

```
....
97.   public String add(HttpServletRequest request, ModelMap
model,String sxid) {
....
106.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1846:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1846
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	129	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String save(String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
129.                    String content,String nextUrl,
HttpServletRequest request,
....
140.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1847:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1847
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String save(String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
129.                    String content,String nextUrl,
HttpServletRequest request,
....
140.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1848:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1848
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String save(String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
129.                    String content,String nextUrl,
HttpServletRequest request,
....
140.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1849:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1849
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String save(String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
129.                    String content,String nextUrl,
HttpServletRequest request,
....
140.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1850:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1850
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String save(String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
129.                    String content,String nextUrl,
HttpServletRequest request,
....
140.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1851:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1851
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	179	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
179.        public String edit(Integer id,HttpServletRequest request,
....
187.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1852:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1852
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	179	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
179.        public String edit(Integer id,HttpServletRequest request,
....
187.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1853:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1853
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	179	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
179.        public String edit(Integer id,HttpServletRequest request,
....
187.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1854:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1854
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	179	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
179.        public String edit(Integer id,HttpServletRequest request,
....
187.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1855:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1855
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	179	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
179.        public String edit(Integer id,HttpServletRequest request,
....
187.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1856:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1856
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	211	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
211.        public String show(Integer id,HttpServletRequest request,
....
219.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1857:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1857
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	211	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
211.        public String show(Integer id,HttpServletRequest request,
....
219.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1858:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1858
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	211	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
211.        public String show(Integer id,HttpServletRequest request,
....
219.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1859:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1859
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	211	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
211.        public String show(Integer id,HttpServletRequest request,
....
219.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1860:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1860
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	211	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
211.        public String show(Integer id,HttpServletRequest request,
....
219.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1861:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1861
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	238	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String update(Integer id,String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
238.                    String content,String nextUrl,
HttpServletRequest request,
....
249.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1862:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1862
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	238	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String update(Integer id,String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
238.                    String content,String nextUrl,
HttpServletRequest request,
....
249.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1863:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1863
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	238	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String update(Integer id,String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
238.                    String content,String nextUrl,
HttpServletRequest request,
....
249.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1864:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1864
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	238	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String update(Integer id,String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
238.                    String content,String nextUrl,
HttpServletRequest request,
....
249.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1865:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1865
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	238	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String update(Integer id,String maintitle, String departmentid,String wszx_captcha,String sxid,String sxmc,

```
....
238.                    String content,String nextUrl,
HttpServletRequest request,
....
249.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1866:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1866
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	273	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
273.        public String delete(Integer id, HttpServletRequest request,
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1867:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1867
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	273	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
273.        public String delete(Integer id, HttpServletRequest request,
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1868:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1868
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	273	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
273.        public String delete(Integer id, HttpServletRequest request,
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1869:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1869
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	273	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
273.        public String delete(Integer id, HttpServletRequest request,
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1870:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1870
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	273	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/AdvisoryAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
273.        public String delete(Integer id, HttpServletRequest request,
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1871:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1871
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	79	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
79.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
87.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1872:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1872
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	79	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
79.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
87.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1873:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1873
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	79	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
79.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
87.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1874:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1874
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	79	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
79.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
87.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1875:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1875
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	79	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
79.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
87.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1876:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1876
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	114	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String news_comments(Integer pageNo, HttpServletRequest request,

```
....
114.        public String news_comments(Integer pageNo,
HttpServletRequest request,
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1877:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1877
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	114	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String news_comments(Integer pageNo, HttpServletRequest request,

```
....
114.        public String news_comments(Integer pageNo,
HttpServletRequest request,
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1878:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1878
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	114	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String news_comments(Integer pageNo, HttpServletRequest request,

```
....
114.        public String news_comments(Integer pageNo,
HttpServletRequest request,
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1879:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1879
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	114	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String news_comments(Integer pageNo, HttpServletRequest request,

```
....
114.        public String news_comments(Integer pageNo,
HttpServletRequest request,
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1880:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1880
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	114	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String news_comments(Integer pageNo, HttpServletRequest request,

```
....
114.        public String news_comments(Integer pageNo,
HttpServletRequest request,
....
122.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1881:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1881
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	147	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String delete(Integer commentId, Integer userId, String ip,

```
....
147.                    Integer pageNo, String nextUrl,
HttpServletRequest request,
....
155.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1882:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1882
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	147	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String delete(Integer commentId, Integer userId, String ip,

```
....
147.                    Integer pageNo, String nextUrl,
HttpServletRequest request,
....
155.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1883:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1883
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	147	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String delete(Integer commentId, Integer userId, String ip,

```
....
147.                    Integer pageNo, String nextUrl,
HttpServletRequest request,
....
155.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1884:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1884
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	147	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String delete(Integer commentId, Integer userId, String ip,

```
....
147.                    Integer pageNo, String nextUrl,
HttpServletRequest request,
....
155.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1885:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1885
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	147	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String delete(Integer commentId, Integer userId, String ip,

```
....
147.                    Integer pageNo, String nextUrl,
HttpServletRequest request,
....
155.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1886:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1886
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	70	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String list(String queryTitle, Integer queryChannelId,

```
....
70.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
77.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1887:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1887
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	70	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String list(String queryTitle, Integer queryChannelId,

```
....
70.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
77.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1888:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1888
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	70	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String list(String queryTitle, Integer queryChannelId,

```
....
70.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
77.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1889:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1889
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	70	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String list(String queryTitle, Integer queryChannelId,

```
....
70.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
77.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1890:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1890
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	70	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String list(String queryTitle, Integer queryChannelId,

```
....
70.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
77.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1891:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1891
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	103	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String add(HttpServletRequest request, ModelMap model) {

```
....
103.        public String add(HttpServletRequest request, ModelMap
model) {
....
110.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1892:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1892
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String add(HttpServletRequest request, ModelMap model) {

```
....
103.        public String add(HttpServletRequest request, ModelMap
model) {
....
110.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1893:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1893
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String add(HttpServletRequest request, ModelMap model) {

```
....
103.        public String add(HttpServletRequest request, ModelMap
model) {
....
110.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1894:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1894
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String add(HttpServletRequest request, ModelMap model) {

```
....
103.        public String add(HttpServletRequest request, ModelMap
model) {
....
110.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1895:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1895
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String add(HttpServletRequest request, ModelMap model) {

```
....
103.        public String add(HttpServletRequest request, ModelMap
model) {
....
110.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1896:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1896
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	202	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String edit(Integer id, HttpServletRequest request,

```
....
202.        public String edit(Integer id, HttpServletRequest request,
....
210.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1897:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1897
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	202	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String edit(Integer id, HttpServletRequest request,

```
....
202.        public String edit(Integer id, HttpServletRequest request,
....
210.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1898:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1898
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	202	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String edit(Integer id, HttpServletRequest request,

```
....
202.        public String edit(Integer id, HttpServletRequest request,
....
210.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1899:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1899
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	202	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String edit(Integer id, HttpServletRequest request,

```
....
202.        public String edit(Integer id, HttpServletRequest request,
....
210.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1900:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1900
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	202	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String edit(Integer id, HttpServletRequest request,

```
....
202.        public String edit(Integer id, HttpServletRequest request,
....
210.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1901:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1901
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	258	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String update(Integer id, String title, String author,

```
....
258.                    String nextUrl, HttpServletRequest request,
....
266.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1902:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1902
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	258	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String update(Integer id, String title, String author,

```
....
258.                    String nextUrl, HttpServletRequest request,
....
266.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1903:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1903
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	258	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String update(Integer id, String title, String author,

```
....
258.                    String nextUrl, HttpServletRequest request,
....
266.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1904:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1904
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	258	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String update(Integer id, String title, String author,

```
....
258.                    String nextUrl, HttpServletRequest request,
....
266.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1905:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1905
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	258	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String update(Integer id, String title, String author,

```
....
258.                    String nextUrl, HttpServletRequest request,
....
266.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1906:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1906
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	305	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String delete(Integer[] ids, HttpServletRequest request,

```
....
305.        public String delete(Integer[] ids, HttpServletRequest
request,
....
313.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1907:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1907
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	305	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String delete(Integer[] ids, HttpServletRequest request,

```
....
305.        public String delete(Integer[] ids, HttpServletRequest
request,
....
313.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1908:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1908
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	305	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String delete(Integer[] ids, HttpServletRequest request,

```
....
305.        public String delete(Integer[] ids, HttpServletRequest
request,
....
313.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1909:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1909
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	305	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String delete(Integer[] ids, HttpServletRequest request,

```
....
305.        public String delete(Integer[] ids, HttpServletRequest
request,
....
313.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1910:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1910
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	305	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String delete(Integer[] ids, HttpServletRequest request,

```
....
305.        public String delete(Integer[] ids, HttpServletRequest
request,
....
313.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1911:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1911
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	51	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public String collection_list(String queryTitle, Integer queryChannelId,

```
....
51.                 Integer pageNo, HttpServletRequest request,
....
59.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1912:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1912
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public String collection_list(String queryTitle, Integer queryChannelId,

```
....
51.               Integer pageNo, HttpServletRequest request,
....
59.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1913:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1913
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public String collection_list(String queryTitle, Integer queryChannelId,

```
....
51.                 Integer pageNo, HttpServletRequest request,
....
59.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1914:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1914
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public String collection_list(String queryTitle, Integer queryChannelId,

```
....
51.                 Integer pageNo, HttpServletRequest request,
....
59.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1915:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1915
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public String collection_list(String queryTitle, Integer queryChannelId,

```
....
51.                 Integer pageNo, HttpServletRequest request,
....
59.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1916:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1916
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	55	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String mycomments(Integer pageNo, HttpServletRequest request,

```
....
55.   public String mycomments(Integer pageNo, HttpServletRequest
request,
....
63.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1917:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1917
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String mycomments(Integer pageNo, HttpServletRequest request,

```
....
55.   public String mycomments(Integer pageNo, HttpServletRequest
request,
....
63.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1918:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1918
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String mycomments(Integer pageNo, HttpServletRequest request,

```
....
55.   public String mycomments(Integer pageNo, HttpServletRequest
request,
....
63.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1919:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1919
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String mycomments(Integer pageNo, HttpServletRequest request,

```
....
55.   public String mycomments(Integer pageNo, HttpServletRequest
request,
....
63.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1920:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1920
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CommentMemberAct.java

方法 public String mycomments(Integer pageNo, HttpServletRequest request,

```
....
55.   public String mycomments(Integer pageNo, HttpServletRequest
request,
....
63.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1921:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1921
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	47	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1922:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1922
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	47	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.               HttpServletRequest request, ModelMap model) {
....
58.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1923:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1923
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	47	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1924:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1924
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	47	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1925:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1925
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	47	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1926:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1926
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	47	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1927:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1927
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	47	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.               HttpServletRequest request, ModelMap model) {
....
58.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1928:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1928
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	47	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1929:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1929
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	47	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1930:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1930
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	47	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageCutActgr.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
47.                HttpServletRequest request, ModelMap model) {
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1931:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1931
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	63	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java

方法 public String execute(

```
....
63.                HttpServletRequest request, ModelMap model) {
....
70.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1932:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1932
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	63	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java

方法 public String execute(

```
....
63.               HttpServletRequest request, ModelMap model) {
....
70.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1933:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1933
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	63	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java

方法 public String execute(

```
....
63.                HttpServletRequest request, ModelMap model) {
....
70.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1934:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1934
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	63	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java

方法 public String execute(

```
....
63.                HttpServletRequest request, ModelMap model) {
....
70.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1935:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1935
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	63	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadAct.java

方法 public String execute(

```
....
63.                HttpServletRequest request, ModelMap model) {
....
70.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1936:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1936
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	62	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
....
69.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1937:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1937
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java

方法 public String execute(

```
....
62.               HttpServletRequest request, ModelMap model) {
....
69.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1938:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1938
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
....
69.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1939:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1939
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
....
69.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1940:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1940
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseImageUploadActgr.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
....
69.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1941:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1941
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	50	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String myguestbook(Integer pageNo, Integer ctgId,

```
....
50.                HttpServletRequest request, HttpServletResponse
response,
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1942:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1942
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	50	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String myguestbook(Integer pageNo, Integer ctgId,

```
....
50.               HttpServletRequest request, HttpServletResponse
response,
....
58.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1943:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1943
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	50	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String myguestbook(Integer pageNo, Integer ctgId,

```
....
50.                HttpServletRequest request, HttpServletResponse
response,
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1944:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1944
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	50	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String myguestbook(Integer pageNo, Integer ctgId,

```
....
50.                HttpServletRequest request, HttpServletResponse
response,
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1945:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1945
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	50	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String myguestbook(Integer pageNo, Integer ctgId,

```
....
50.                HttpServletRequest request, HttpServletResponse
response,
....
58.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1946:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1946
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	76	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_detail(Integer id, HttpServletRequest request,

```
....
76.   public String guestbook_detail(Integer id, HttpServletRequest
request,
....
84.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1947:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1947
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_detail(Integer id, HttpServletRequest request,

```
....
76.   public String guestbook_detail(Integer id, HttpServletRequest
request,
....
84.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1948:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1948
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_detail(Integer id, HttpServletRequest request,

```
....
76.   public String guestbook_detail(Integer id, HttpServletRequest
request,
....
84.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1949:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1949
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_detail(Integer id, HttpServletRequest request,

```
....
76.   public String guestbook_detail(Integer id, HttpServletRequest
request,
....
84.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1950:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1950
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_detail(Integer id, HttpServletRequest request,

```
....
76.   public String guestbook_detail(Integer id, HttpServletRequest
request,
....
84.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1951:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1951
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	99	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
99.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
107.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1952:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1952
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	99	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
99.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
107.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1953:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1953
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	99	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
99.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
107.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1954:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1954
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	99	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
99.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
107.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1955:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1955
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	99	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/GuestbookMemberAct.java

方法 public String guestbook_replay(Integer id, String nextUrl,HttpServletRequest request,

```
....
99.   public String guestbook_replay(Integer id, String
nextUrl,HttpServletRequest request,
....
107.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1956:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1956
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	46	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
46.                HttpServletRequest request, ModelMap model) {
....
57.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1957:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1957
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	46	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
46.               HttpServletRequest request, ModelMap model) {
....
57.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1958:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1958
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	46	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
46.                 HttpServletRequest request, ModelMap model) {
....
57.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1959:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1959
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
46.                HttpServletRequest request, ModelMap model) {
....
57.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1960:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1960
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageCutAct.java

方法 public String imageAreaSelect(String uploadBase, String imgSrcPath,

```
....
46.                 HttpServletRequest request, ModelMap model) {
....
57.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1961:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1961
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	62	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
63.          String onlyShowURL = (String)
request.getParameter("onlyShowURL");
....
73.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1962:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1962
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java

方法 public String execute(

```
....
62.               HttpServletRequest request, ModelMap model) {
63.         String onlyShowURL = (String)
request.getParameter("onlyShowURL");
....
73.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1963:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1963
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	62	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
63.          String onlyShowURL = (String)
request.getParameter("onlyShowURL");
....
73.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1964:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1964
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
63.          String onlyShowURL = (String)
request.getParameter("onlyShowURL");
....
73.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1965:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1965
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	62	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ImageUploadAct.java

方法 public String execute(

```
....
62.                HttpServletRequest request, ModelMap model) {
63.          String onlyShowURL = (String)
request.getParameter("onlyShowURL");
....
73.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1966:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1966
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	69	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String index(HttpServletRequest request,

```
....
69.   public String index(HttpServletRequest request,
....
73.         String sxid = request.getParameter("sxid") == null ? "" :
request.getParameter("sxid");
....
86.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1967:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1967
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String index(HttpServletRequest request,

```
....
69.   public String index(HttpServletRequest request,
....
73.         String sxid = request.getParameter("sxid") == null ? "" :
request.getParameter("sxid");
....
86.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1968:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1968
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String index(HttpServletRequest request,

```
....
69.   public String index(HttpServletRequest request,
....
73.         String sxid = request.getParameter("sxid") == null ? "" :
request.getParameter("sxid");
....
86.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1969:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1969
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String index(HttpServletRequest request,

```
....
69.   public String index(HttpServletRequest request,
....
73.         String sxid = request.getParameter("sxid") == null ? "" :
request.getParameter("sxid");
....
86.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1970:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1970
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String index(HttpServletRequest request,

```
....
69.   public String index(HttpServletRequest request,
....
73.         String sxid = request.getParameter("sxid") == null ? "" :
request.getParameter("sxid");
....
86.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1971:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1971
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	107	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
107.        public String profileInput(HttpServletRequest request,
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1972:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1972
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	107	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
107.        public String profileInput(HttpServletRequest request,
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1973:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1973
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	107	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
107.        public String profileInput(HttpServletRequest request,
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1974:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1974
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	107	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
107.        public String profileInput(HttpServletRequest request,
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1975:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1975
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	107	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileInput(HttpServletRequest request,

```
....
107.        public String profileInput(HttpServletRequest request,
....
121.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1976:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1976
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	137	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String portrait(HttpServletRequest request,

```
....
137.        public String portrait(HttpServletRequest request,
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1977:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1977
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	137	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String portrait(HttpServletRequest request,

```
....
137.        public String portrait(HttpServletRequest request,
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1978:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1978
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	137	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String portrait(HttpServletRequest request,

```
....
137.        public String portrait(HttpServletRequest request,
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1979:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1979
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	137	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String portrait(HttpServletRequest request,

```
....
137.        public String portrait(HttpServletRequest request,
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1980:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1980
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	137	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String portrait(HttpServletRequest request,

```
....
137.        public String portrait(HttpServletRequest request,
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1981:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1981
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	262	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
262.        public String passwordInput(HttpServletRequest request,
....
275.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1982:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1982
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	262	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
262.        public String passwordInput(HttpServletRequest request,
....
275.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1983:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1983
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	262	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
262.        public String passwordInput(HttpServletRequest request,
....
275.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1984:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1984
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	262	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
262.        public String passwordInput(HttpServletRequest request,
....
275.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1985:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1985
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	262	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
262.        public String passwordInput(HttpServletRequest request,
....
275.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1986:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1986
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	303	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
303.                    String nextUrl, HttpServletRequest request,
....
311.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1987:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1987
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	303	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
303.                    String nextUrl, HttpServletRequest request,
....
311.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1988:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1988
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	303	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
303.                    String nextUrl, HttpServletRequest request,
....
311.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1989:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1989
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	303	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
303.                    String nextUrl, HttpServletRequest request,
....
311.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1990:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1990
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	303	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordSubmit(String origPwd, String newPwd, String email,

```
....
303.                    String nextUrl, HttpServletRequest request,
....
311.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1991:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1991
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	335	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoInput(HttpServletRequest request,

```
....
335.        public String peopleInfoInput(HttpServletRequest request,
....
343.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1992:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1992
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	335	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoInput(HttpServletRequest request,

```
....
335.        public String peopleInfoInput(HttpServletRequest request,
....
343.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1993:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1993
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	335	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoInput(HttpServletRequest request,

```
....
335.        public String peopleInfoInput(HttpServletRequest request,
....
343.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1994:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1994
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	335	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoInput(HttpServletRequest request,

```
....
335.        public String peopleInfoInput(HttpServletRequest request,
....
343.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 1995:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1995
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	335	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoInput(HttpServletRequest request,

```
....
335.        public String peopleInfoInput(HttpServletRequest request,
....
343.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1996:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1996
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	375	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoSubmit(THrUser tHrUser,

```
....
375.                    String nextUrl, HttpServletRequest request,
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 1997:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1997
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	375	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoSubmit(THrUser tHrUser,

```
....
375.                    String nextUrl, HttpServletRequest request,
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 1998:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1998
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	375	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoSubmit(THrUser tHrUser,

```
....
375.                    String nextUrl, HttpServletRequest request,
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 1999:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1999
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	375	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoSubmit(THrUser tHrUser,

```
....
375.                    String nextUrl, HttpServletRequest request,
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2000:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2000
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	375	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String peopleInfoSubmit(THrUser tHrUser,

```
....
375.                    String nextUrl, HttpServletRequest request,
....
383.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

▼

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2001:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2001
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	76	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_mng(Integer box, String msg,

```
....
76.                HttpServletRequest request, HttpServletResponse
response,
....
84.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2002:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2002
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_mng(Integer box, String msg,

```
....
76.               HttpServletRequest request, HttpServletResponse
response,
....
84.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2003:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2003
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_mng(Integer box, String msg,

```
....
76.                HttpServletRequest request, HttpServletResponse
response,
....
84.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2004:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2004
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_mng(Integer box, String msg,

```
....
76.                HttpServletRequest request, HttpServletResponse
response,
....
84.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2005:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2005
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_mng(Integer box, String msg,

```
....
76.                HttpServletRequest request, HttpServletResponse
response,
....
84.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2006:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2006
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	118	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_inbox(Integer pageNo, String title,

```
....
118.                    HttpServletRequest request, HttpServletResponse
response,
....
126.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2007:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2007
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	118	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_inbox(Integer pageNo, String title,

```
....
118.                    HttpServletRequest request, HttpServletResponse
response,
....
126.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2008:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2008
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	118	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_inbox(Integer pageNo, String title,

```
....
118.                    HttpServletRequest request, HttpServletResponse
response,
....
126.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2009:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2009
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	118	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_inbox(Integer pageNo, String title,

```
....
118.                    HttpServletRequest request, HttpServletResponse
response,
....
126.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2010:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2010
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	118	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_inbox(Integer pageNo, String title,

```
....
118.                    HttpServletRequest request, HttpServletResponse
response,
....
126.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2011:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2011
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	171	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_add(HttpServletRequest request,

```
....
171.        public String message_add(HttpServletRequest request,
....
179.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2012:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2012
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	171	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_add(HttpServletRequest request,

```
....
171.        public String message_add(HttpServletRequest request,
....
179.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2013:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2013
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	171	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_add(HttpServletRequest request,

```
....
171.        public String message_add(HttpServletRequest request,
....
179.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2014:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2014
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	171	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_add(HttpServletRequest request,

```
....
171.        public String message_add(HttpServletRequest request,
....
179.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2015:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2015
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	171	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_add(HttpServletRequest request,

```
....
171.        public String message_add(HttpServletRequest request,
....
179.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2016:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2016
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	189	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_reply(Integer id, HttpServletRequest request,

```
....
189.        public String message_reply(Integer id, HttpServletRequest
request,
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2017:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2017
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	189	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_reply(Integer id, HttpServletRequest request,

```
....
189.        public String message_reply(Integer id, HttpServletRequest
request,
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2018:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2018
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	189	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_reply(Integer id, HttpServletRequest request,

```
....
189.        public String message_reply(Integer id, HttpServletRequest
request,
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2019:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2019
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	189	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_reply(Integer id, HttpServletRequest request,

```
....
189.        public String message_reply(Integer id, HttpServletRequest
request,
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2020:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2020
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	189	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_reply(Integer id, HttpServletRequest request,

```
....
189.        public String message_reply(Integer id, HttpServletRequest
request,
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2021:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2021
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	332	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_edit(Integer id, HttpServletRequest request,

```
....
332.        public String message_edit(Integer id, HttpServletRequest
request,
....
340.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2022:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2022
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	332	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_edit(Integer id, HttpServletRequest request,

```
....
332.        public String message_edit(Integer id, HttpServletRequest
request,
....
340.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2023:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2023
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	332	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_edit(Integer id, HttpServletRequest request,

```
....
332.        public String message_edit(Integer id, HttpServletRequest
request,
....
340.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2024:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2024
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	332	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_edit(Integer id, HttpServletRequest request,

```
....
332.        public String message_edit(Integer id, HttpServletRequest
request,
....
340.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2025:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2025
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	332	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_edit(Integer id, HttpServletRequest request,

```
....
332.        public String message_edit(Integer id, HttpServletRequest
request,
....
340.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2026:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2026
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	397	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_read(Integer id, Integer box,

```
....
397.                    HttpServletRequest request, HttpServletResponse
response,
....
405.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2027:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2027
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	397	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_read(Integer id, Integer box,

```
....
397.                    HttpServletRequest request, HttpServletResponse
response,
....
405.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2028:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2028
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	397	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_read(Integer id, Integer box,

```
....
397.                    HttpServletRequest request, HttpServletResponse
response,
....
405.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2029:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2029
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	397	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_read(Integer id, Integer box,

```
....
397.                    HttpServletRequest request, HttpServletResponse
response,
....
405.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2030:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2030
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	397	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_read(Integer id, Integer box,

```
....
397.                    HttpServletRequest request, HttpServletResponse
response,
....
405.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2031:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2031
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	442	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_forward(Integer id, HttpServletRequest request,

```
....
442.        public String message_forward(Integer id, HttpServletRequest
request,
....
450.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2032:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2032
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	442	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_forward(Integer id, HttpServletRequest request,

```
....
442.        public String message_forward(Integer id, HttpServletRequest
request,
....
450.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2033:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2033
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	442	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_forward(Integer id, HttpServletRequest request,

```
....
442.        public String message_forward(Integer id, HttpServletRequest
request,
....
450.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2034:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2034
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	442	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_forward(Integer id, HttpServletRequest request,

```
....
442.        public String message_forward(Integer id, HttpServletRequest
request,
....
450.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2035:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2035
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	442	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_forward(Integer id, HttpServletRequest request,

```
....
442.        public String message_forward(Integer id, HttpServletRequest
request,
....
450.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2036:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2036
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	636	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_delete(Integer[] ids, String nextUrl,

```
....
636.                    HttpServletRequest request, HttpServletResponse
response,
....
644.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2037:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2037
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	636	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_delete(Integer[] ids, String nextUrl,

```
....
636.                    HttpServletRequest request, HttpServletResponse
response,
....
644.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2038:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2038
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	636	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_delete(Integer[] ids, String nextUrl,

```
....
636.                    HttpServletRequest request, HttpServletResponse
response,
....
644.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2039:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2039
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	636	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_delete(Integer[] ids, String nextUrl,

```
....
636.                    HttpServletRequest request, HttpServletResponse
response,
....
644.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2040:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2040
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	636	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String message_delete(Integer[] ids, String nextUrl,

```
....
636.                    HttpServletRequest request, HttpServletResponse
response,
....
644.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2041:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2041
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	165	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
165.                    HttpServletRequest request, HttpServletResponse
response,
....
173.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2042:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2042
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	165	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
165.                    HttpServletRequest request, HttpServletResponse
response,
....
173.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2043:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2043
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	165	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
165.                    HttpServletRequest request, HttpServletResponse
response,
....
173.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2044:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2044
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	165	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
165.                    HttpServletRequest request, HttpServletResponse
response,
....
173.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2045:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2045
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	165	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String profileSubmit(CmsUserExt ext, String nextUrl,

```
....
165.                    HttpServletRequest request, HttpServletResponse
response,
....
173.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2046:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2046
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	73	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String wssbpermlist(String deptid, String deptname,

```
....
73.                 String permid, String permname, String permtype,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
85.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2047:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2047
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	73	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String wssbpermlist(String deptid, String deptname,

```
....
73.                 String permid, String permname, String permtype,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
85.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2048:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2048
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	73	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String wssbpermlist(String deptid, String deptname,

```
....
73.                 String permid, String permname, String permtype,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
85.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2049:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2049
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	73	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String wssbpermlist(String deptid, String deptname,

```
....
73.                 String permid, String permname, String permtype,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
85.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2050:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2050
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	73	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String wssbpermlist(String deptid, String deptname,

```
....
73.                 String permid, String permname, String permtype,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
85.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2051:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2051
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	80	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String list(String queryTitle, String deptId,

```
....
80.                Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
92.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2052:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2052
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	80	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String list(String queryTitle, String deptId,

```
....
80.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
92.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2053:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2053
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	80	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String list(String queryTitle, String deptId,

```
....
80.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
92.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2054:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2054
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	80	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String list(String queryTitle, String deptId,

```
....
80.                Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
92.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2055:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2055
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	80	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String list(String queryTitle, String deptId,

```
....
80.                 Integer pageNo, HttpServletRequest request, ModelMap
model) {
....
92.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2056:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2056
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	118	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String add(String deptid,HttpServletRequest request, ModelMap model) {

```
....
118.        public String add(String deptid,HttpServletRequest request,
ModelMap model) {
....
130.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2057:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2057
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	118	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String add(String deptid,HttpServletRequest request, ModelMap model) {

```
....
118.        public String add(String deptid,HttpServletRequest request,
ModelMap model) {
....
130.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2058:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2058
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	118	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String add(String deptid,HttpServletRequest request, ModelMap model) {

```
....
118.        public String add(String deptid,HttpServletRequest request,
ModelMap model) {
....
130.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2059:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2059
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	118	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String add(String deptid,HttpServletRequest request, ModelMap model) {

```
....
118.        public String add(String deptid,HttpServletRequest request,
ModelMap model) {
....
130.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2060:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2060
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	118	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String add(String deptid,HttpServletRequest request, ModelMap model) {

```
....
118.        public String add(String deptid,HttpServletRequest request,
ModelMap model) {
....
130.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2061:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2061
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	151	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String save(String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String name,String wsts_captcha,

```
....
151.                    String content,String nextUrl,
HttpServletRequest request,
....
162.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2062:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2062
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String save(String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String name,String wsts_captcha,

```
....
151.                    String content,String nextUrl,
HttpServletRequest request,
....
162.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2063:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2063
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	151	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String save(String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String name,String wsts_captcha,

```
....
151.                    String content,String nextUrl,
HttpServletRequest request,
....
162.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2064:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2064
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String save(String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String name,String wsts_captcha,

```
....
151.                    String content,String nextUrl,
HttpServletRequest request,
....
162.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2065:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2065
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	151	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String save(String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String name,String wsts_captcha,

```
....
151.                    String content,String nextUrl,
HttpServletRequest request,
....
162.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2066:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2066
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	203	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
203.        public String edit(Integer id,HttpServletRequest request,
....
211.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2067:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2067
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	203	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
203.        public String edit(Integer id,HttpServletRequest request,
....
211.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2068:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2068
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	203	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
203.        public String edit(Integer id,HttpServletRequest request,
....
211.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2069:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2069
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	203	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
203.        public String edit(Integer id,HttpServletRequest request,
....
211.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2070:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2070
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	203	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String edit(Integer id,HttpServletRequest request,

```
....
203.        public String edit(Integer id,HttpServletRequest request,
....
211.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2071:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2071
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	234	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
234.        public String show(Integer id,HttpServletRequest request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2072:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2072
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
234.        public String show(Integer id,HttpServletRequest request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2073:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2073
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
234.        public String show(Integer id,HttpServletRequest request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2074:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2074
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
234.        public String show(Integer id,HttpServletRequest request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2075:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2075
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
234.        public String show(Integer id,HttpServletRequest request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2076:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2076
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	302	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
302.        public String delete(Integer id, HttpServletRequest request,
....
310.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2077:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2077
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	302	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
302.        public String delete(Integer id, HttpServletRequest request,
....
310.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2078:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2078
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	302	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
302.        public String delete(Integer id, HttpServletRequest request,
....
310.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2079:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2079
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	302	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
302.        public String delete(Integer id, HttpServletRequest request,
....
310.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2080:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2080
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	302	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String delete(Integer id, HttpServletRequest request,

```
....
302.        public String delete(Integer id, HttpServletRequest request,
....
310.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2081:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2081
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	102	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String input(HttpServletRequest request,

```
....
102.        public String input(HttpServletRequest request,
....
112.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2082:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2082
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	102	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String input(HttpServletRequest request,

```
....
102.        public String input(HttpServletRequest request,
....
112.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2083:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2083
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	102	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String input(HttpServletRequest request,

```
....
102.        public String input(HttpServletRequest request,
....
112.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2084:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2084
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	102	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String input(HttpServletRequest request,

```
....
102.        public String input(HttpServletRequest request,
....
112.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2085:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2085
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	102	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String input(HttpServletRequest request,

```
....
102.        public String input(HttpServletRequest request,
....
112.                    return FrontUtils.showMessage(request, model,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2086:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2086
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	66	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String zihaochachong(String pnum,String rtype,Integer pageNo,HttpServletRequest request, ModelMap model){

```
....
66.   public String zihaochachong(String pnum,String rtype,Integer
pageNo,HttpServletRequest request, ModelMap model){
....
73.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2087:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2087
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	66	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String zihaochachong(String pnum,String rtype,Integer pageNo,HttpServletRequest request, ModelMap model){

```
....
66.   public String zihaochachong(String pnum,String rtype,Integer
pageNo,HttpServletRequest request, ModelMap model){
....
73.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2088:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2088
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	66	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String zihaochachong(String pnum,String rtype,Integer pageNo,HttpServletRequest request, ModelMap model){

```
....
66.   public String zihaochachong(String pnum,String rtype,Integer
pageNo,HttpServletRequest request, ModelMap model){
....
73.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2089:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2089
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	66	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String zihaochachong(String pnum,String rtype,Integer pageNo,HttpServletRequest request, ModelMap model){

```
....
66.   public String zihaochachong(String pnum,String rtype,Integer
pageNo,HttpServletRequest request, ModelMap model){
....
73.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2090:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2090
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	66	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String zihaochachong(String pnum,String rtype,Integer pageNo,HttpServletRequest request, ModelMap model){

```
....
66.   public String zihaochachong(String pnum,String rtype,Integer
pageNo,HttpServletRequest request, ModelMap model){
....
73.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2091:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2091
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	261	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String update(Integer id,String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String wsts_captcha,

```
....
261.                    String content,String nextUrl,
HttpServletRequest request,
....
272.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2092:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2092
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	261	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String update(Integer id,String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String wsts_captcha,

```
....
261.                    String content,String nextUrl,
HttpServletRequest request,
....
272.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2093:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2093
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	261	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String update(Integer id,String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String wsts_captcha,

```
....
261.                    String content,String nextUrl,
HttpServletRequest request,
....
272.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2094:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2094
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	261	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String update(Integer id,String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String wsts_captcha,

```
....
261.                    String content,String nextUrl,
HttpServletRequest request,
....
272.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2095:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2095
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	261	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReferComplainAct.java

方法 public String update(Integer id,String becomplainedname,String becomplainedsex,String departmentid,String becomplainedduty,String maintitle, String wsts_captcha,

```
....
261.                    String content,String nextUrl,
HttpServletRequest request,
....
272.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2096:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2096
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	176	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
183.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2097:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2097
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	176	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
183.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2098:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2098
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	176	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
183.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2099:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2099
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	176	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
183.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2100:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2100
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	176	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
183.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2101:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2101
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	68	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String list(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
68.   public String list(Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
75.                return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2102:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2102
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	68	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String list(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
68.   public String list(Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
75.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2103:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2103
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	68	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String list(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
68.   public String list(Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
75.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2104:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2104
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	68	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String list(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
68.   public String list(Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
75.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2105:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2105
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	68	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String list(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
68.   public String list(Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
75.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2106:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2106
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	87	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(HttpServletRequest request, ModelMap model) throws Exception {

```
....
87.   public String add(HttpServletRequest request, ModelMap model)
throws Exception {
....
94.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2107:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2107
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	87	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(HttpServletRequest request, ModelMap model) throws Exception {

```
....
87.   public String add(HttpServletRequest request, ModelMap model)
throws Exception {
....
94.               return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2108:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2108
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	87	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(HttpServletRequest request, ModelMap model) throws Exception {

```
....
87.   public String add(HttpServletRequest request, ModelMap model)
throws Exception {
....
94.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2109:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2109
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	87	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(HttpServletRequest request, ModelMap model) throws Exception {

```
....
87.   public String add(HttpServletRequest request, ModelMap model)
throws Exception {
....
94.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2110:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2110
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	87	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(HttpServletRequest request, ModelMap model) throws Exception {

```
....
87.   public String add(HttpServletRequest request, ModelMap model)
throws Exception {
....
94.                 return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2111:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2111
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	109	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(String bsnum,HttpServletRequest request, ModelMap model) throws Exception {

```
....
109.        public String add(String bsnum,HttpServletRequest request,
ModelMap model) throws Exception {
....
116.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2112:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2112
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	109	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(String bsnum,HttpServletRequest request, ModelMap model) throws Exception {

```
....
109.        public String add(String bsnum,HttpServletRequest request,
ModelMap model) throws Exception {
....
116.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2113:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2113
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	109	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(String bsnum,HttpServletRequest request, ModelMap model) throws Exception {

```
....
109.        public String add(String bsnum,HttpServletRequest request,
ModelMap model) throws Exception {
....
116.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2114:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2114
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	109	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(String bsnum,HttpServletRequest request, ModelMap model) throws Exception {

```
....
109.        public String add(String bsnum,HttpServletRequest request,
ModelMap model) throws Exception {
....
116.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2115:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2115
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	109	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String add(String bsnum,HttpServletRequest request, ModelMap model) throws Exception {

```
....
109.        public String add(String bsnum,HttpServletRequest request,
ModelMap model) throws Exception {
....
116.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2116:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2116
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	183	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
183.                    String content,String nextUrl,
HttpServletRequest request,
....
191.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2117:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2117
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	183	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
183.                    String content,String nextUrl,
HttpServletRequest request,
....
191.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2118:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2118
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	183	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
183.                    String content,String nextUrl,
HttpServletRequest request,
....
191.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2119:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2119
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	183	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
183.                    String content,String nextUrl,
HttpServletRequest request,
....
191.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2120:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2120
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	183	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String save(String departmentid,String permissionitemId,String bsnum,String createtime,

```
....
183.                    String content,String nextUrl,
HttpServletRequest request,
....
191.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2121:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2121
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	234	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String viewPrint(String bsnum,HttpServletRequest request,

```
....
234.        public String viewPrint(String bsnum,HttpServletRequest
request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2122:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2122
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String viewPrint(String bsnum,HttpServletRequest request,

```
....
234.        public String viewPrint(String bsnum,HttpServletRequest
request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2123:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2123
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String viewPrint(String bsnum,HttpServletRequest request,

```
....
234.        public String viewPrint(String bsnum,HttpServletRequest
request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2124:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2124
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String viewPrint(String bsnum,HttpServletRequest request,

```
....
234.        public String viewPrint(String bsnum,HttpServletRequest
request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2125:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2125
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public String viewPrint(String bsnum,HttpServletRequest request,

```
....
234.        public String viewPrint(String bsnum,HttpServletRequest
request,
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2126:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2126
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	243	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String list(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
243.      public String list(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
244.          Res res = new Res(request, model, SPACE_LIST);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2127:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2127
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	243	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String list(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
243.      public String list(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
244.          Res res = new Res(request, model, SPACE_LIST);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2128:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2128
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	243	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String list(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
243.      public String list(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
244.          Res res = new Res(request, model, SPACE_LIST);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2129:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2129
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	243	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String list(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
243.      public String list(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
244.          Res res = new Res(request, model, SPACE_LIST);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2130:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2130
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	243	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String list(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
243.      public String list(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
244.          Res res = new Res(request, model, SPACE_LIST);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2131:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2131
结果评论	
被分配给	

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	279	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String profileSubmit(TWebHallUserInforMation userInfo, TWebHallIncInforMation inc,

```
....
279.              HttpServletRequest request, HttpServletResponse
response, ModelMap model) {
280.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2132:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2132
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	279	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String profileSubmit(TWebHallUserInforMation userInfo, TWebHallIncInforMation inc,

```
....
279.              HttpServletRequest request, HttpServletResponse
response, ModelMap model) {
280.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2133:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2133
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	279	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String profileSubmit(TWebHallUserInforMation userInfo, TWebHallIncInforMation inc,

```
....
279.                HttpServletRequest request, HttpServletResponse
response, ModelMap model) {
280.            Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.               public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2134:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2134
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	279	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String profileSubmit(TWebHallUserInforMation userInfo, TWebHallIncInforMation inc,

```
....
279.              HttpServletRequest request, HttpServletResponse
response, ModelMap model) {
280.          Res res = new Res(request, model, null);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2135:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2135
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	279	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String profileSubmit(TWebHallUserInforMation userInfo, TWebHallIncInforMation inc,

```
....
279.              HttpServletRequest request, HttpServletResponse
response, ModelMap model) {
280.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2136:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2136
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	346	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String shareUpdate(String values, HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
346.      public String shareUpdate(String values, HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
347.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2137:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2137
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	346	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String shareUpdate(String values, HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
346.      public String shareUpdate(String values, HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
347.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2138:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2138
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	346	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String shareUpdate(String values, HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
346.      public String shareUpdate(String values, HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
347.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2139:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2139
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String shareUpdate(String values, HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
346.      public String shareUpdate(String values, HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
347.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2140:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2140
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	346	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String shareUpdate(String values, HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
346.      public String shareUpdate(String values, HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
347.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2141:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2141
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	396	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String findAll(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
396.      public String findAll(Integer pageNo, HttpServletRequest
request, ModelMap model) {
397.          Res res = new Res(request, model, SPACE_HISINFO);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2142:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2142
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	396	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAll(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
396.      public String findAll(Integer pageNo, HttpServletRequest
request, ModelMap model) {
397.          Res res = new Res(request, model, SPACE_HISINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2143:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2143
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	396	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String findAll(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
396.      public String findAll(Integer pageNo, HttpServletRequest
request, ModelMap model) {
397.          Res res = new Res(request, model, SPACE_HISINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2144:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2144
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	396	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String findAll(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
396.      public String findAll(Integer pageNo, HttpServletRequest
request, ModelMap model) {
397.          Res res = new Res(request, model, SPACE_HISINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2145:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2145
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	396	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAll(Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
396.      public String findAll(Integer pageNo, HttpServletRequest
request, ModelMap model) {
397.          Res res = new Res(request, model, SPACE_HISINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2146:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2146
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	432	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String getCertInfoHis(String certCode, HttpServletRequest request, ModelMap model) {

```
....
432.      public String getCertInfoHis(String certCode,
HttpServletRequest request, ModelMap model) {
433.          Res res = new Res(request, model, SPACE_HISCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2147:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2147
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	432	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String getCertInfoHis(String certCode, HttpServletRequest request, ModelMap model) {

```
....
432.      public String getCertInfoHis(String certCode,
HttpServletRequest request, ModelMap model) {
433.          Res res = new Res(request, model, SPACE_HISCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2148:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2148
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	432	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String getCertInfoHis(String certCode, HttpServletRequest request, ModelMap model) {

```
....
432.      public String getCertInfoHis(String certCode,
HttpServletRequest request, ModelMap model) {
433.          Res res = new Res(request, model, SPACE_HISCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2149:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2149
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	432	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String getCertInfoHis(String certCode, HttpServletRequest request, ModelMap model) {

```
....
432.      public String getCertInfoHis(String certCode,
HttpServletRequest request, ModelMap model) {
433.          Res res = new Res(request, model, SPACE_HISCERT);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2150:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2150
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	432	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String getCertInfoHis(String certCode, HttpServletRequest request, ModelMap model) {

```
....
432.      public String getCertInfoHis(String certCode,
HttpServletRequest request, ModelMap model) {
433.          Res res = new Res(request, model, SPACE_HISCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2151:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2151
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	447	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String findAttachInfo(Integer pageNo, String type, String clmc, HttpServletRequest request, ModelMap model) {

```
....
447.      public String findAttachInfo(Integer pageNo, String type,
String clmc, HttpServletRequest request, ModelMap model) {
....
452.              res = new Res(request, model, SPACE_CERTINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2152:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2152
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	447	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAttachInfo(Integer pageNo, String type, String clmc, HttpServletRequest request, ModelMap model) {

```
....
447.      public String findAttachInfo(Integer pageNo, String type,
String clmc, HttpServletRequest request, ModelMap model) {
....
452.              res = new Res(request, model, SPACE_CERTINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2153:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2153
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	447	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAttachInfo(Integer pageNo, String type, String clmc, HttpServletRequest request, ModelMap model) {

```
....
447.      public String findAttachInfo(Integer pageNo, String type,
String clmc, HttpServletRequest request, ModelMap model) {
....
452.              res = new Res(request, model, SPACE_CERTINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2154:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2154
结果评论	
被分配给	

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	447	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAttachInfo(Integer pageNo, String type, String clmc, HttpServletRequest request, ModelMap model) {

```
....
447.      public String findAttachInfo(Integer pageNo, String type,
String clmc, HttpServletRequest request, ModelMap model) {
....
452.              res = new Res(request, model, SPACE_CERTINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2155:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2155
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	447	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String findAttachInfo(Integer pageNo, String type, String clmc, HttpServletRequest request, ModelMap model) {

```
....
447.      public String findAttachInfo(Integer pageNo, String type,
String clmc, HttpServletRequest request, ModelMap model) {
....
452.                res = new Res(request, model, SPACE_CERTINFO);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.               public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2156:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2156
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	483	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String getAttachHis(String clbh, String userCode, Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
483.      public String getAttachHis(String clbh, String userCode,
Integer pageNo, HttpServletRequest request, ModelMap model) {
484.          Res res = new Res(request, model, SPACE_HISATTACH);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2157:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2157
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	483	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String getAttachHis(String clbh, String userCode, Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
483.      public String getAttachHis(String clbh, String userCode,
Integer pageNo, HttpServletRequest request, ModelMap model) {
484.          Res res = new Res(request, model, SPACE_HISATTACH);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2158:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2158
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	483	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String getAttachHis(String clbh, String userCode, Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
483.      public String getAttachHis(String clbh, String userCode,
Integer pageNo, HttpServletRequest request, ModelMap model) {
484.          Res res = new Res(request, model, SPACE_HISATTACH);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2159:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2159
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	483	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public String getAttachHis(String clbh, String userCode, Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
483.      public String getAttachHis(String clbh, String userCode,
Integer pageNo, HttpServletRequest request, ModelMap model) {
484.          Res res = new Res(request, model, SPACE_HISATTACH);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2160:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2160
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	483	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String getAttachHis(String clbh, String userCode, Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
483.      public String getAttachHis(String clbh, String userCode,
Integer pageNo, HttpServletRequest request, ModelMap model) {
484.          Res res = new Res(request, model, SPACE_HISATTACH);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2161:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2161
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	507	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
507.      public String spaceAdd(String type, HttpServletRequest
request, ModelMap model) {
....
512.              res = new Res(request, model, SPACE_UPLOADCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2162:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2162
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	507	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
507.      public String spaceAdd(String type, HttpServletRequest
request, ModelMap model) {
....
512.              res = new Res(request, model, SPACE_UPLOADCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2163:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2163
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	507	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
507.      public String spaceAdd(String type, HttpServletRequest
request, ModelMap model) {
....
512.                res = new Res(request, model, SPACE_UPLOADCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.               public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2164:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2164
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	507	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spaceAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
507.      public String spaceAdd(String type, HttpServletRequest
request, ModelMap model) {
....
512.              res = new Res(request, model, SPACE_UPLOADCERT);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2165:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2165
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	507	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spaceAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
507.      public String spaceAdd(String type, HttpServletRequest
request, ModelMap model) {
....
512.              res = new Res(request, model, SPACE_UPLOADCERT);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2166:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2166
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	682	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
684.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2167:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2167
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	682	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
684.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2168:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2168
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	682	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
684.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                         setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2169:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2169
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	682	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
684.          Res res = new Res(request, model, null);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2170:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2170
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	682	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
682.      public String spacedeptlist(String areaId, String type,
HttpServletRequest request, HttpServletResponse response,
....
684.          Res res = new Res(request, model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2171:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2171
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	790	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacepermlist(String sxid, String clmc, String type, Integer pageNo, HttpServletRequest request,

```
....
790.      public String spacepermlist(String sxid, String clmc, String
type, Integer pageNo, HttpServletRequest request,
....
792.          Res res = new Res(request, model, SPACE_SPACEMAIN);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2172:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2172
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	790	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacepermlist(String sxid, String clmc, String type, Integer pageNo, HttpServletRequest request,

```
....
790.      public String spacepermlist(String sxid, String clmc, String
type, Integer pageNo, HttpServletRequest request,
....
792.          Res res = new Res(request, model, SPACE_SPACEMAIN);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2173:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2173
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	790	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacepermlist(String sxid, String clmc, String type, Integer pageNo, HttpServletRequest request,

```
....
790.      public String spacepermlist(String sxid, String clmc, String
type, Integer pageNo, HttpServletRequest request,
....
792.          Res res = new Res(request, model, SPACE_SPACEMAIN);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                         setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2174:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2174
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	790	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacepermlist(String sxid, String clmc, String type, Integer pageNo, HttpServletRequest request,

```
....
790.      public String spacepermlist(String sxid, String clmc, String
type, Integer pageNo, HttpServletRequest request,
....
792.          Res res = new Res(request, model, SPACE_SPACEMAIN);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2175:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2175
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	790	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacepermlist(String sxid, String clmc, String type, Integer pageNo, HttpServletRequest request,

```
....
790.      public String spacepermlist(String sxid, String clmc, String
type, Integer pageNo, HttpServletRequest request,
....
792.          Res res = new Res(request, model, SPACE_SPACEMAIN);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2176:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2176
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	835	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAttachAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
835.      public String spaceAttachAdd(String type, HttpServletRequest
request, ModelMap model) {
....
840.              res = new Res(request, model, SPACE_UPLOADCERT_ADD);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2177:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2177
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	835	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAttachAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
835.      public String spaceAttachAdd(String type, HttpServletRequest
request, ModelMap model) {
....
840.              res = new Res(request, model, SPACE_UPLOADCERT_ADD);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2178:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2178
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	835	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spaceAttachAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
835.      public String spaceAttachAdd(String type, HttpServletRequest
request, ModelMap model) {
....
840.                res = new Res(request, model, SPACE_UPLOADCERT_ADD);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.               public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2179:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2179
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	835	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spaceAttachAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
835.      public String spaceAttachAdd(String type, HttpServletRequest
request, ModelMap model) {
....
840.              res = new Res(request, model, SPACE_UPLOADCERT_ADD);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                          setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2180:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2180
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	835	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spaceAttachAdd(String type, HttpServletRequest request, ModelMap model) {

```
....
835.      public String spaceAttachAdd(String type, HttpServletRequest
request, ModelMap model) {
....
840.              res = new Res(request, model, SPACE_UPLOADCERT_ADD);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public Res(HttpServletRequest request, Map<String, Object> model, String name) {

```
....
1005.             public Res(HttpServletRequest request, Map<String,
Object> model, String name) {
....
1012.                           setUrl(FrontUtils.showMessage(request,
model, "member.memberClose"));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2181:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2181
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	75	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zaibanjianlist(String bsnum, String permname,

```
....
75.                String starttime, String endtime, String deptname,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
78.          UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
100.                     return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2182:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2182
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	75	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zaibanjianlist(String bsnum, String permname,

```
....
75.                String starttime, String endtime, String deptname,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
78.          UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
100.                     return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2183:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2183
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	75	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String zaibanjianlist(String bsnum, String permname,

```
....
75.                String starttime, String endtime, String deptname,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
78.          UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
100.                     return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.               String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.               Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2184:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2184
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	75	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String zaibanjianlist(String bsnum, String permname,

```
....
75.                String starttime, String endtime, String deptname,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
78.          UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
100.                     return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.               String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.               Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2185:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2185
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	75	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String zaibanjianlist(String bsnum, String permname,

```
....
75.                String starttime, String endtime, String deptname,
Integer pageNo, HttpServletRequest request, ModelMap model) {
....
78.          UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
100.                     return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.               frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.               Long startTime = (Long)
request.getAttribute(START_TIME);
325.               String areaId = request.getParameter("areaId");
....
327.               if(areaId != null && !areaId.equals("")){
....
329.                     if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.               String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.               Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2186:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2186
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	129	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String banjiejianlist(String bsnum, String permname,

```
....
129.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
132.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2187:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2187
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String banjiejianlist(String bsnum, String permname,

```
....
129.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
132.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2188:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2188
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String banjiejianlist(String bsnum, String permname,

```
....
129.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
132.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2189:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2189
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String banjiejianlist(String bsnum, String permname,

```
....
129.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
132.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2190:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2190
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String banjiejianlist(String bsnum, String permname,

```
....
129.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
132.              UnifiedUser users =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
145.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2191:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2191
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	182	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String zancunjianlist(String bsnum, String permname,

```
....
182.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2192:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2192
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	182	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zancunjianlist(String bsnum, String permname,

```
....
182.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2193:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2193
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	182	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zancunjianlist(String bsnum, String permname,

```
....
182.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2194:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2194
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zancunjianlist(String bsnum, String permname,

```
....
182.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2195:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2195
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String zancunjianlist(String bsnum, String permname,

```
....
182.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
197.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2196:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2196
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	227	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String tuihuijianlist(String bsnum, String permname,

```
....
227.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2197:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2197
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	227	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String tuihuijianlist(String bsnum, String permname,

```
....
227.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2198:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2198
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	227	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String tuihuijianlist(String bsnum, String permname,

```
....
227.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2199:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2199
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	227	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String tuihuijianlist(String bsnum, String permname,

```
....
227.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2200:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2200
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	227	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String tuihuijianlist(String bsnum, String permname,

```
....
227.                    String starttime, String endtime, String
deptname, Integer pageNo, HttpServletRequest request, ModelMap model) {
....
242.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2201:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2201
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	196	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
196.                    String deptId,HttpServletRequest request,
ModelMap model){
....
203.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2202:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2202
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	196	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
196.                    String deptId,HttpServletRequest request,
ModelMap model){
....
203.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2203:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2203
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	196	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
196.                    String deptId,HttpServletRequest request,
ModelMap model){
....
203.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2204:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2204
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	196	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
196.                    String deptId,HttpServletRequest request,
ModelMap model){
....
203.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2205:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2205
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	196	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String areaId,

```
....
196.                    String deptId,HttpServletRequest request,
ModelMap model){
....
203.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2206:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2206
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	238	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
238.                    String deptId,HttpServletRequest request,
ModelMap model){
....
245.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2207:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2207
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	238	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
238.                    String deptId,HttpServletRequest request,
ModelMap model){
....
245.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2208:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2208
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	238	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
238.                    String deptId,HttpServletRequest request,
ModelMap model){
....
245.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2209:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2209
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	238	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
238.                    String deptId,HttpServletRequest request,
ModelMap model){
....
245.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2210:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2210
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	238	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String areaId,

```
....
238.                    String deptId,HttpServletRequest request,
ModelMap model){
....
245.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2211:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2211
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	274	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
274.                    String deptId,HttpServletRequest request,
ModelMap model){
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2212:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2212
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	274	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
274.                    String deptId,HttpServletRequest request,
ModelMap model){
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2213:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2213
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	274	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
274.                    String deptId,HttpServletRequest request,
ModelMap model){
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2214:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2214
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	274	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
274.                    String deptId,HttpServletRequest request,
ModelMap model){
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2215:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2215
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	274	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
274.                    String deptId,HttpServletRequest request,
ModelMap model){
....
281.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2216:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2216
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	405	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
405.                    String deptId,HttpServletRequest request,
ModelMap model){
....
412.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2217:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2217
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	405	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
405.                    String deptId,HttpServletRequest request,
ModelMap model){
....
412.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2218:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2218
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	405	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
405.                    String deptId,HttpServletRequest request,
ModelMap model){
....
412.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2219:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2219
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	405	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
405.                    String deptId,HttpServletRequest request,
ModelMap model){
....
412.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2220:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2220
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	405	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
405.                    String deptId,HttpServletRequest request,
ModelMap model){
....
412.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2221:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2221
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	192	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
192.                    String deptId,HttpServletRequest request,
ModelMap model){
....
199.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2222:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2222
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	192	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
192.                    String deptId,HttpServletRequest request,
ModelMap model){
....
199.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2223:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2223
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	192	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
192.                    String deptId,HttpServletRequest request,
ModelMap model){
....
199.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2224:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2224
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	192	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
192.                    String deptId,HttpServletRequest request,
ModelMap model){
....
199.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2225:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2225
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	192	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
192.                    String deptId,HttpServletRequest request,
ModelMap model){
....
199.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2226:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2226
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	234	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
234.                    String deptId,HttpServletRequest request,
ModelMap model){
....
241.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2227:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2227
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
234.                    String deptId,HttpServletRequest request,
ModelMap model){
....
241.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2228:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2228
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	234	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
234.                    String deptId,HttpServletRequest request,
ModelMap model){
....
241.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2229:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2229
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
234.                    String deptId,HttpServletRequest request,
ModelMap model){
....
241.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2230:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2230
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	234	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
234.                    String deptId,HttpServletRequest request,
ModelMap model){
....
241.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2231:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2231
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	270	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
270.                    String deptId,HttpServletRequest request,
ModelMap model){
....
277.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2232:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2232
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	270	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
270.                    String deptId,HttpServletRequest request,
ModelMap model){
....
277.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2233:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2233
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	270	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
270.                    String deptId,HttpServletRequest request,
ModelMap model){
....
277.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2234:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2234
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	270	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
270.                    String deptId,HttpServletRequest request,
ModelMap model){
....
277.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2235:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2235
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	270	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,

```
....
270.                    String deptId,HttpServletRequest request,
ModelMap model){
....
277.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2236:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2236
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	313	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
313.                    String deptId,HttpServletRequest request,
ModelMap model){
....
320.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2237:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2237
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	313	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
313.                    String deptId,HttpServletRequest request,
ModelMap model){
....
320.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2238:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2238
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	313	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
313.                    String deptId,HttpServletRequest request,
ModelMap model){
....
320.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2239:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2239
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	313	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
313.                    String deptId,HttpServletRequest request,
ModelMap model){
....
320.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2240:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2240
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	313	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String enterpriseSsDeptCancelStorePermBySxid(String sxid,String sxzxname,String fcode,String sortcode,String areaId,

```
....
313.                    String deptId,HttpServletRequest request,
ModelMap model){
....
320.                    return FrontUtils.showMessage(request, model,
"member.memberClose");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showMessage(HttpServletRequest request,

```
....
265.        public static String showMessage(HttpServletRequest request,
....
268.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2241:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2241
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	69	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String list(Integer siteId, Integer contentId, Integer greatTo,

```
....
69.                 HttpServletRequest request, HttpServletResponse
response,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2242:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2242
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String list(Integer siteId, Integer contentId, Integer greatTo,

```
....
69.                 HttpServletRequest request, HttpServletResponse
response,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2243:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2243
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	69	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String list(Integer siteId, Integer contentId, Integer greatTo,

```
....
69.                 HttpServletRequest request, HttpServletResponse
response,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2244:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2244
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java
方法	public String list(Integer siteId, Integer contentId, Integer greatTo,

```
....
69.                HttpServletRequest request, HttpServletResponse
response,
....
97.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.         public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.    public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.          return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2245:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2245
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CommentAct.java

方法 public String list(Integer siteId, Integer contentId, Integer greatTo,

```
....
69.               HttpServletRequest request, HttpServletResponse
response,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2246:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2246
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	51	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
51.   public String toHdjl( HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2247:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2247
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
51.   public String toHdjl( HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2248:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2248
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java
方法	public String toHdjl(HttpServletRequest request,

```
....
51.   public String toHdjl( HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2249:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2249
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
51.   public String toHdjl( HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2250:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2250
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ContactUsAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
51.   public String toHdjl( HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2251:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2251
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	41	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java

方法 public String custom(String tpl, HttpServletRequest request,

```
....
41.   public String custom(String tpl, HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2252:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2252
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java

方法 public String custom(String tpl, HttpServletRequest request,

```
....
41.   public String custom(String tpl, HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2253:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2253
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java
方法	public String custom(String tpl, HttpServletRequest request,

```
....
41.   public String custom(String tpl, HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2254:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2254
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java

方法 public String custom(String tpl, HttpServletRequest request,

```
....
41.   public String custom(String tpl, HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2255:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2255
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/CsiCustomAct.java

方法 public String custom(String tpl, HttpServletRequest request,

```
....
41.   public String custom(String tpl, HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2256:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2256
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	369	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2(HttpServletRequest request, ModelMap model) {

```
....
369.        public String index2(HttpServletRequest request, ModelMap
model) {
....
371.                String region = request.getParameter("service");
....
383.                String pagewd = request.getParameter("pagewd");
....
391.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2257:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2257
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	369	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2(HttpServletRequest request, ModelMap model) {

```
....
369.        public String index2(HttpServletRequest request, ModelMap
model) {
....
371.                String region = request.getParameter("service");
....
383.                String pagewd = request.getParameter("pagewd");
....
391.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2258:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2258
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	369	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2(HttpServletRequest request, ModelMap model) {

```
....
369.        public String index2(HttpServletRequest request, ModelMap
model) {
....
371.                String region = request.getParameter("service");
....
383.                String pagewd = request.getParameter("pagewd");
....
391.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2259:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2259
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	369	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index2(HttpServletRequest request, ModelMap model) {

```
....
369.        public String index2(HttpServletRequest request, ModelMap
model) {
....
371.                String region = request.getParameter("service");
....
383.                String pagewd = request.getParameter("pagewd");
....
391.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2260:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2260
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	369	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index2(HttpServletRequest request, ModelMap model) {

```
....
369.        public String index2(HttpServletRequest request, ModelMap
model) {
....
371.                String region = request.getParameter("service");
....
383.                String pagewd = request.getParameter("pagewd");
....
391.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2261:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2261
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	396	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index5(HttpServletRequest request, ModelMap model) {

```
....
396.        public String index5(HttpServletRequest request, ModelMap
model) {
....
398.                String region = request.getParameter("service");
....
410.                String pagewd = request.getParameter("pagewd");
....
418.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2262:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2262
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	396	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index5(HttpServletRequest request, ModelMap model) {

```
....
396.        public String index5(HttpServletRequest request, ModelMap
model) {
....
398.                String region = request.getParameter("service");
....
410.                String pagewd = request.getParameter("pagewd");
....
418.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2263:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2263
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	396	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index5(HttpServletRequest request, ModelMap model) {

```
....
396.        public String index5(HttpServletRequest request, ModelMap
model) {
....
398.              String region = request.getParameter("service");
....
410.              String pagewd = request.getParameter("pagewd");
....
418.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2264:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2264
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	396	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index5(HttpServletRequest request, ModelMap model) {

```
....
396.        public String index5(HttpServletRequest request, ModelMap
model) {
....
398.                String region = request.getParameter("service");
....
410.                String pagewd = request.getParameter("pagewd");
....
418.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2265:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2265
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	396	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index5(HttpServletRequest request, ModelMap model) {

```
....
396.        public String index5(HttpServletRequest request, ModelMap
model) {
....
398.                String region = request.getParameter("service");
....
410.                String pagewd = request.getParameter("pagewd");
....
418.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2266:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2266
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	423	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybs(HttpServletRequest request, ModelMap model) {

```
....
423.        public String wybs(HttpServletRequest request, ModelMap
model) {
....
425.                String region = request.getParameter("service");
....
440.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2267:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2267
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	423	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybs(HttpServletRequest request, ModelMap model) {

```
....
423.        public String wybs(HttpServletRequest request, ModelMap
model) {
....
425.                String region = request.getParameter("service");
....
440.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2268:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2268
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	423	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybs(HttpServletRequest request, ModelMap model) {

```
....
423.        public String wybs(HttpServletRequest request, ModelMap
model) {
....
425.                String region = request.getParameter("service");
....
440.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2269:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2269
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	423	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String wybs(HttpServletRequest request, ModelMap model) {

```
....
423.        public String wybs(HttpServletRequest request, ModelMap
model) {
....
425.                String region = request.getParameter("service");
....
440.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2270:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2270
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	423	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybs(HttpServletRequest request, ModelMap model) {

```
....
423.        public String wybs(HttpServletRequest request, ModelMap
model) {
....
425.                String region = request.getParameter("service");
....
440.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2271:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2271
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	446	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybsgr(HttpServletRequest request, ModelMap model) {

```
....
446.        public String wybsgr(HttpServletRequest request, ModelMap
model) {
....
448.                String region = request.getParameter("service");
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2272:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2272
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	446	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybsgr(HttpServletRequest request, ModelMap model) {

```
....
446.        public String wybsgr(HttpServletRequest request, ModelMap
model) {
....
448.                String region = request.getParameter("service");
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2273:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2273
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	446	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybsgr(HttpServletRequest request, ModelMap model) {

```
....
446.        public String wybsgr(HttpServletRequest request, ModelMap
model) {
....
448.                String region = request.getParameter("service");
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2274:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2274
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	446	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String wybsgr(HttpServletRequest request, ModelMap model) {

```
....
446.        public String wybsgr(HttpServletRequest request, ModelMap
model) {
....
448.                String region = request.getParameter("service");
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2275:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2275
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	446	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String wybsgr(HttpServletRequest request, ModelMap model) {

```
....
446.        public String wybsgr(HttpServletRequest request, ModelMap
model) {
....
448.                String region = request.getParameter("service");
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2276:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2276
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	469	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index3(HttpServletRequest request, ModelMap model) {

```
....
469.        public String index3(HttpServletRequest request, ModelMap
model) {
....
471.                String region = request.getParameter("service");
....
482.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2277:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2277
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	469	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index3(HttpServletRequest request, ModelMap model) {

```
....
469.        public String index3(HttpServletRequest request, ModelMap
model) {
....
471.                String region = request.getParameter("service");
....
482.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2278:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2278
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	469	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index3(HttpServletRequest request, ModelMap model) {

```
....
469.        public String index3(HttpServletRequest request, ModelMap
model) {
....
471.              String region = request.getParameter("service");
....
482.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2279:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2279
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	469	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index3(HttpServletRequest request, ModelMap model) {

```
....
469.        public String index3(HttpServletRequest request, ModelMap
model) {
....
471.                String region = request.getParameter("service");
....
482.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2280:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2280
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	469	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index3(HttpServletRequest request, ModelMap model) {

```
....
469.        public String index3(HttpServletRequest request, ModelMap
model) {
....
471.                String region = request.getParameter("service");
....
482.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2281:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2281
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	51	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String adspace(Integer id, HttpServletRequest request,

```
....
51.   public String adspace(Integer id, HttpServletRequest request,
....
60.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2282:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2282
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String adspace(Integer id, HttpServletRequest request,

```
....
51.   public String adspace(Integer id, HttpServletRequest request,
....
60.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2283:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2283
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	51	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String adspace(Integer id, HttpServletRequest request,

```
....
51.   public String adspace(Integer id, HttpServletRequest request,
....
60.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2284:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2284
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java
方法	public String adspace(Integer id, HttpServletRequest request,

```
....
51.   public String adspace(Integer id, HttpServletRequest request,
....
60.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2285:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2285
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AdvertisingAct.java

方法 public String adspace(Integer id, HttpServletRequest request,

```
....
51.   public String adspace(Integer id, HttpServletRequest request,
....
60.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2286:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2286
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	586	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2_1(HttpServletRequest request, ModelMap model) {

```
....
586.        public String index2_1(HttpServletRequest request, ModelMap
model) {
....
588.                String region = request.getParameter("service");
....
597.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2287:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2287
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	586	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2_1(HttpServletRequest request, ModelMap model) {

```
....
586.        public String index2_1(HttpServletRequest request, ModelMap
model) {
....
588.                String region = request.getParameter("service");
....
597.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2288:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2288
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	586	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String index2_1(HttpServletRequest request, ModelMap model) {

```
....
586.        public String index2_1(HttpServletRequest request, ModelMap
model) {
....
588.                String region = request.getParameter("service");
....
597.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2289:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2289
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	586	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index2_1(HttpServletRequest request, ModelMap model) {

```
....
586.        public String index2_1(HttpServletRequest request, ModelMap
model) {
....
588.                String region = request.getParameter("service");
....
597.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2290:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2290
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	586	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String index2_1(HttpServletRequest request, ModelMap model) {

```
....
586.        public String index2_1(HttpServletRequest request, ModelMap
model) {
....
588.                String region = request.getParameter("service");
....
597.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2291:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2291
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	603	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian(HttpServletRequest request, ModelMap model) {

```
....
603.        public String banjian(HttpServletRequest request, ModelMap
model) {
....
605.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2292:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2292
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	603	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian(HttpServletRequest request, ModelMap model) {

```
....
603.        public String banjian(HttpServletRequest request, ModelMap
model) {
....
605.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2293:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2293
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	603	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian(HttpServletRequest request, ModelMap model) {

```
....
603.        public String banjian(HttpServletRequest request, ModelMap
model) {
....
605.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2294:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2294
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	603	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String banjian(HttpServletRequest request, ModelMap model) {

```
....
603.        public String banjian(HttpServletRequest request, ModelMap
model) {
....
605.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2295:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2295
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	603	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String banjian(HttpServletRequest request, ModelMap model) {

```
....
603.        public String banjian(HttpServletRequest request, ModelMap
model) {
....
605.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2296:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2296
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	611	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian2(HttpServletRequest request, ModelMap model) {

```
....
611.        public String banjian2(HttpServletRequest request, ModelMap
model) {
....
613.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2297:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2297
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	611	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian2(HttpServletRequest request, ModelMap model) {

```
....
611.        public String banjian2(HttpServletRequest request, ModelMap
model) {
....
613.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2298:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2298
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	611	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian2(HttpServletRequest request, ModelMap model) {

```
....
611.        public String banjian2(HttpServletRequest request, ModelMap
model) {
....
613.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2299:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2299
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	611	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String banjian2(HttpServletRequest request, ModelMap model) {

```
....
611.        public String banjian2(HttpServletRequest request, ModelMap
model) {
....
613.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2300:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2300
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	611	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String banjian2(HttpServletRequest request, ModelMap model) {

```
....
611.        public String banjian2(HttpServletRequest request, ModelMap
model) {
....
613.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2301:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2301
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	449	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
449.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
452.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
454.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2302:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2302
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	449	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
449.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
452.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
454.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2303:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2303
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	449	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
449.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
452.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
454.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2304:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2304
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	449	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
449.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
452.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
454.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2305:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2305
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	449	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
449.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
452.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
454.                        return FrontUtils.pageNotFound(request,
response, model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2306:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2306
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	558	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
558.        public String download(@PathVariable String id,
HttpServletRequest request,
....
562.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2307:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2307
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	558	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
558.        public String download(@PathVariable String id,
HttpServletRequest request,
....
562.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2308:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2308
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	558	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
558.        public String download(@PathVariable String id,
HttpServletRequest request,
....
562.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2309:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2309
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	558	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
558.        public String download(@PathVariable String id,
HttpServletRequest request,
....
562.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2310:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2310
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	558	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
558.        public String download(@PathVariable String id,
HttpServletRequest request,
....
562.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2311:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2311
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	434	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法 public String printcl(HttpServletRequest request,

```
....
434.        public String printcl( HttpServletRequest request,
....
437.                String id = request.getParameter("id");
....
439.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2312:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2312
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	434	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String printcl(HttpServletRequest request,

```
....
434.        public String printcl( HttpServletRequest request,
....
437.              String id = request.getParameter("id");
....
439.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2313:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2313
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	434	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String printcl(HttpServletRequest request,

```
....
434.        public String printcl( HttpServletRequest request,
....
437.                String id = request.getParameter("id");
....
439.                      return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2314:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2314
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	434	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String printcl(HttpServletRequest request,

```
....
434.        public String printcl( HttpServletRequest request,
....
437.                String id = request.getParameter("id");
....
439.                      return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2315:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2315
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	434	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String printcl(HttpServletRequest request,

```
....
434.        public String printcl( HttpServletRequest request,
....
437.              String id = request.getParameter("id");
....
439.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2316:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2316
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	895	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_tjzj(@PathVariable String id, HttpServletRequest request,

```
....
895.        public String wssb_tjzj(@PathVariable String id,
HttpServletRequest request,
....
899.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2317:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2317
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	895	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_tjzj(@PathVariable String id, HttpServletRequest request,

```
....
895.        public String wssb_tjzj(@PathVariable String id,
HttpServletRequest request,
....
899.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2318:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2318
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	895	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_tjzj(@PathVariable String id, HttpServletRequest request,

```
....
895.        public String wssb_tjzj(@PathVariable String id,
HttpServletRequest request,
....
899.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2319:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2319
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	895	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_tjzj(@PathVariable String id, HttpServletRequest request,

```
....
895.        public String wssb_tjzj(@PathVariable String id,
HttpServletRequest request,
....
899.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2320:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2320
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	895	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_tjzj(@PathVariable String id, HttpServletRequest request,

```
....
895.        public String wssb_tjzj(@PathVariable String id,
HttpServletRequest request,
....
899.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2321:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2321
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	913	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_bdtj(@PathVariable String id, HttpServletRequest request,

```
....
913.        public String wssb_bdtj(@PathVariable String id,
HttpServletRequest request,
....
917.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2322:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2322
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	913	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_bdtj(@PathVariable String id, HttpServletRequest request,

```
....
913.        public String wssb_bdtj(@PathVariable String id,
HttpServletRequest request,
....
917.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2323:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2323
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	913	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_bdtj(@PathVariable String id, HttpServletRequest request,

```
....
913.        public String wssb_bdtj(@PathVariable String id,
HttpServletRequest request,
....
917.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2324:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2324
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	913	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_bdtj(@PathVariable String id, HttpServletRequest request,

```
....
913.        public String wssb_bdtj(@PathVariable String id,
HttpServletRequest request,
....
917.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2325:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2325
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	913	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_bdtj(@PathVariable String id, HttpServletRequest request,

```
....
913.        public String wssb_bdtj(@PathVariable String id,
HttpServletRequest request,
....
917.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2326:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2326
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	931	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_scfj(@PathVariable String id, HttpServletRequest request,

```
....
931.        public String wssb_scfj(@PathVariable String id,
HttpServletRequest request,
....
935.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2327:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2327
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	931	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_scfj(@PathVariable String id, HttpServletRequest request,

```
....
931.        public String wssb_scfj(@PathVariable String id,
HttpServletRequest request,
....
935.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2328:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2328
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	931	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_scfj(@PathVariable String id, HttpServletRequest request,

```
....
931.        public String wssb_scfj(@PathVariable String id,
HttpServletRequest request,
....
935.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2329:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2329
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	931	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_scfj(@PathVariable String id, HttpServletRequest request,

```
....
931.        public String wssb_scfj(@PathVariable String id,
HttpServletRequest request,
....
935.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2330:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2330
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	931	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_scfj(@PathVariable String id, HttpServletRequest request,

```
....
931.        public String wssb_scfj(@PathVariable String id,
HttpServletRequest request,
....
935.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2331:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2331
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	967	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_sqsb(@PathVariable String id, HttpServletRequest request,

```
....
967.        public String wssb_sqsb(@PathVariable String id,
HttpServletRequest request,
....
971.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2332:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2332
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	967	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_sqsb(@PathVariable String id, HttpServletRequest request,

```
....
967.        public String wssb_sqsb(@PathVariable String id,
HttpServletRequest request,
....
971.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2333:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2333
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	967	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_sqsb(@PathVariable String id, HttpServletRequest request,

```
....
967.        public String wssb_sqsb(@PathVariable String id,
HttpServletRequest request,
....
971.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2334:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2334
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	967	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_sqsb(@PathVariable String id, HttpServletRequest request,

```
....
967.        public String wssb_sqsb(@PathVariable String id,
HttpServletRequest request,
....
971.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2335:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2335
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	967	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_sqsb(@PathVariable String id, HttpServletRequest request,

```
....
967.        public String wssb_sqsb(@PathVariable String id,
HttpServletRequest request,
....
971.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2336:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2336
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1106	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法 public String zhenjieshow(HttpServletRequest request,

```
....
1106.       public String zhenjieshow(HttpServletRequest request,
....
1110.               String areaId = request.getParameter("areaid");
....
1114.                           return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2337:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2337
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1106	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjieshow(HttpServletRequest request,

```
....
1106.       public String zhenjieshow(HttpServletRequest request,
....
1110.             String areaId = request.getParameter("areaid");
....
1114.                         return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2338:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2338
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1106	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjieshow(HttpServletRequest request,

```
....
1106.       public String zhenjieshow(HttpServletRequest request,
....
1110.               String areaId = request.getParameter("areaid");
....
1114.                           return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2339:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2339
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1106	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjieshow(HttpServletRequest request,

```
....
1106.       public String zhenjieshow(HttpServletRequest request,
....
1110.               String areaId = request.getParameter("areaid");
....
1114.                           return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2340:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2340
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1106	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjieshow(HttpServletRequest request,

```
....
1106.       public String zhenjieshow(HttpServletRequest request,
....
1110.             String areaId = request.getParameter("areaid");
....
1114.                         return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2341:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2341
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1122	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhnejiedesp(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
1122.       public String zhnejiedesp(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
1125.               String areaId = request.getParameter("areaid");
....
1128.                           return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2342:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2342
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1122	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhnejiedesp(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
1122.       public String zhnejiedesp(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
1125.             String areaId = request.getParameter("areaid");
....
1128.                         return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2343:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2343
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1122	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhnejiedesp(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
1122.       public String zhnejiedesp(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
1125.             String areaId = request.getParameter("areaid");
....
1128.                         return FrontUtils.pageNotFound(request,
response, model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2344:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2344
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1122	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhnejiedesp(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
1122.       public String zhnejiedesp(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
1125.               String areaId = request.getParameter("areaid");
....
1128.                           return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2345:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2345
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1122	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhnejiedesp(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
1122.       public String zhnejiedesp(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
1125.             String areaId = request.getParameter("areaid");
....
1128.                         return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2346:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2346
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1136	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1136.       public String zhenjie_baoan(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1141.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1145.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2347:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2347
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1136	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1136.       public String zhenjie_baoan(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1141.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1145.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2348:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2348
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1136	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1136.       public String zhenjie_baoan(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1141.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1145.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2349:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2349
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1136	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1136.       public String zhenjie_baoan(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1141.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1145.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2350:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2350
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1136	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1136.       public String zhenjie_baoan(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1141.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1145.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2351:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2351
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1197	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list_1(String deptId, String permtype,

```
....
1197.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1201.                String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1202.                String sfwssb = request.getParameter("isonline") ==
null ?"0":request.getParameter("isonline");
1203.                String tdtl = request.getParameter("tdtl");
....
1207.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2352:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2352
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1197	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list_1(String deptId, String permtype,

```
....
1197.                   Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1201.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1202.               String sfwssb = request.getParameter("isonline") ==
null ?"0":request.getParameter("isonline");
1203.               String tdtl = request.getParameter("tdtl");
....
1207.                     return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2353:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2353
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1197	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list_1(String deptId, String permtype,

```
....
1197.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1201.                String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1202.                String sfwssb = request.getParameter("isonline") ==
null ?"0":request.getParameter("isonline");
1203.                String tdtl = request.getParameter("tdtl");
....
1207.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2354:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2354
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1197	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list_1(String deptId, String permtype,

```
....
1197.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1201.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1202.              String sfwssb = request.getParameter("isonline") ==
null ?"0":request.getParameter("isonline");
1203.              String tdtl = request.getParameter("tdtl");
....
1207.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2355:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2355
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1197	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_list_1(String deptId, String permtype,

```
....
1197.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1201.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1202.              String sfwssb = request.getParameter("isonline") ==
null ?"0":request.getParameter("isonline");
1203.              String tdtl = request.getParameter("tdtl");
....
1207.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2356:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2356
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1243	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_list_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1243.       public String zhenjie_baoan_list_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1247.             String sqID=request.getParameter("sqID");
....
1251.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1252.             String tdtl = request.getParameter("tdtl");
....
1257.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2357:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2357
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1243	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_list_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1243.       public String zhenjie_baoan_list_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1247.             String sqID=request.getParameter("sqID");
....
1251.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1252.             String tdtl = request.getParameter("tdtl");
....
1257.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2358:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2358
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1243	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_list_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1243.       public String zhenjie_baoan_list_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1247.             String sqID=request.getParameter("sqID");
....
1251.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1252.             String tdtl = request.getParameter("tdtl");
....
1257.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2359:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2359
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1243	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法 public String zhenjie_baoan_list_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1243.       public String zhenjie_baoan_list_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1247.             String sqID=request.getParameter("sqID");
....
1251.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1252.             String tdtl = request.getParameter("tdtl");
....
1257.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2360:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2360
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

行	1243	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1243.       public String zhenjie_baoan_list_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1247.               String sqID=request.getParameter("sqID");
....
1251.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1252.               String tdtl = request.getParameter("tdtl");
....
1257.                     return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2361:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2361
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	949	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_wcsq(@PathVariable String id, HttpServletRequest request,

```
....
949.        public String wssb_wcsq(@PathVariable String id,
HttpServletRequest request,
....
953.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2362:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2362
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	949	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String wssb_wcsq(@PathVariable String id, HttpServletRequest request,

```
....
949.        public String wssb_wcsq(@PathVariable String id,
HttpServletRequest request,
....
953.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2363:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2363
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	949	272
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String wssb_wcsq(@PathVariable String id, HttpServletRequest request,

```
....
949.        public String wssb_wcsq(@PathVariable String id,
HttpServletRequest request,
....
953.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2364:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2364
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	949	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String wssb_wcsq(@PathVariable String id, HttpServletRequest request,

```
....
949.        public String wssb_wcsq(@PathVariable String id,
HttpServletRequest request,
....
953.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2365:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2365
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	949	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String wssb_wcsq(@PathVariable String id, HttpServletRequest request,

```
....
949.        public String wssb_wcsq(@PathVariable String id,
HttpServletRequest request,
....
953.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2366:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2366
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1291	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_1(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1291.       public String zhenjie_baoan_1(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1296.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1297.             String tdtl = request.getParameter("tdtl");
....
1301.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.             frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.             Long startTime = (Long)
request.getAttribute(START_TIME);
325.             String areaId = request.getParameter("areaId");
....
327.             if(areaId != null && !areaId.equals("")){
....
329.                   if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                   Object areaId =
request.getSession().getAttribute("areaId");
....
113.                   List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2367:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2367
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1291	241
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_1(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1291.       public String zhenjie_baoan_1(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1296.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1297.             String tdtl = request.getParameter("tdtl");
....
1301.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.             frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.             Long startTime = (Long)
request.getAttribute(START_TIME);
325.             String areaId = request.getParameter("areaId");
....
327.             if(areaId != null && !areaId.equals("")){
....
329.                   if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.             String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.             Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2368:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2368
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1291	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_1(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1291.       public String zhenjie_baoan_1(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1296.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1297.             String tdtl = request.getParameter("tdtl");
....
1301.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.             frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.             Long startTime = (Long)
request.getAttribute(START_TIME);
325.             String areaId = request.getParameter("areaId");
....
327.             if(areaId != null && !areaId.equals("")){
....
329.                   if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.             String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.             Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2369:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2369
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1291	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_1(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1291.       public String zhenjie_baoan_1(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1296.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1297.             String tdtl = request.getParameter("tdtl");
....
1301.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.             frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.             Long startTime = (Long)
request.getAttribute(START_TIME);
325.             String areaId = request.getParameter("areaId");
....
327.             if(areaId != null && !areaId.equals("")){
....
329.                   if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.             String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.             Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2370:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2370
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1291	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_1(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1291.       public String zhenjie_baoan_1(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1296.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
1297.              String tdtl = request.getParameter("tdtl");
....
1301.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2371:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2371
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1337	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1337.       public String zhenjie_baoan_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1341.             String sqID=request.getParameter("sqID");
1342.             String tdtl = request.getParameter("tdtl");
....
1346.             String deptID  =
request.getParameter("deptID")==null?"1000":request.getParameter("deptID
");
1347.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1352.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2372:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2372
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1337	241
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1337.       public String zhenjie_baoan_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1341.             String sqID=request.getParameter("sqID");
1342.             String tdtl = request.getParameter("tdtl");
....
1346.             String deptID  =
request.getParameter("deptID")==null?"1000":request.getParameter("deptID
");
1347.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1352.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2373:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2373
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1337	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1337.       public String zhenjie_baoan_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1341.               String sqID=request.getParameter("sqID");
1342.               String tdtl = request.getParameter("tdtl");
....
1346.               String deptID  =
request.getParameter("deptID")==null?"1000":request.getParameter("deptID
");
1347.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1352.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2374:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2374
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1337	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1337.       public String zhenjie_baoan_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1341.             String sqID=request.getParameter("sqID");
1342.             String tdtl = request.getParameter("tdtl");
....
1346.             String deptID  =
request.getParameter("deptID")==null?"1000":request.getParameter("deptID
");
1347.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1352.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2375:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2375
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1337	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_2(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1337.       public String zhenjie_baoan_2(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1341.               String sqID=request.getParameter("sqID");
1342.               String tdtl = request.getParameter("tdtl");
....
1346.               String deptID  =
request.getParameter("deptID")==null?"1000":request.getParameter("deptID
");
1347.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1352.                       return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2376:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2376
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1387	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_gxfw(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1387.       public String zhenjie_baoan_gxfw(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1391.               String sqID=request.getParameter("sqID");
....
1395.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1400.                       return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2377:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2377
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1387	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_gxfw(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1387.       public String zhenjie_baoan_gxfw(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1391.             String sqID=request.getParameter("sqID");
....
1395.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1400.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2378:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2378
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1387	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_gxfw(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1387.       public String zhenjie_baoan_gxfw(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1391.               String sqID=request.getParameter("sqID");
....
1395.               String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1400.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2379:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2379
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1387	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_gxfw(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1387.       public String zhenjie_baoan_gxfw(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1391.             String sqID=request.getParameter("sqID");
....
1395.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1400.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2380:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2380
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1387	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_gxfw(HttpServletRequest request,HttpServletResponse response, ModelMap model

```
....
1387.       public String zhenjie_baoan_gxfw(HttpServletRequest
request,HttpServletResponse response, ModelMap model
....
1391.             String sqID=request.getParameter("sqID");
....
1395.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1400.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2381:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2381
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1168	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String zhenjie_baoan_list(String deptId, String permtype,

```
....
1168.                     Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1171.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1174.                     return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2382:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2382
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1168	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list(String deptId, String permtype,

```
....
1168.                   Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1171.             String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1174.                   return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2383:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2383
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1168	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list(String deptId, String permtype,

```
....
1168.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1171.                String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1174.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2384:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2384
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1168	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list(String deptId, String permtype,

```
....
1168.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1171.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1174.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2385:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2385
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1168	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String zhenjie_baoan_list(String deptId, String permtype,

```
....
1168.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
1171.              String parentid  =
request.getParameter("parentid")==null?"1000":request.getParameter("pare
ntid");
....
1174.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2386:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2386
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	41	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String tags(@PathVariable String path, HttpServletRequest request,

```
....
41.   public String tags(@PathVariable String path, HttpServletRequest
request,
....
67.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2387:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2387
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String tags(@PathVariable String path, HttpServletRequest request,

```
....
41.   public String tags(@PathVariable String path, HttpServletRequest
request,
....
67.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2388:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2388
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String tags(@PathVariable String path, HttpServletRequest request,

```
....
41.   public String tags(@PathVariable String path, HttpServletRequest
request,
....
67.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2389:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2389
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String tags(@PathVariable String path, HttpServletRequest request,

```
....
41.   public String tags(@PathVariable String path, HttpServletRequest
request,
....
67.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2390:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2390
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String tags(@PathVariable String path, HttpServletRequest request,

```
....
41.   public String tags(@PathVariable String path, HttpServletRequest
request,
....
67.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2391:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2391
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String index(Integer channelId, Integer topicId,

```
....
35.                HttpServletRequest request, HttpServletResponse
response,
....
58.                      return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2392:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2392
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String index(Integer channelId, Integer topicId,

```
....
35.                 HttpServletRequest request, HttpServletResponse
response,
....
58.                       return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2393:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2393
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String index(Integer channelId, Integer topicId,

```
....
35.                HttpServletRequest request, HttpServletResponse
response,
....
58.                        return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2394:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2394
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String index(Integer channelId, Integer topicId,

```
....
35.                HttpServletRequest request, HttpServletResponse
response,
....
58.                        return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2395:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2395
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String index(Integer channelId, Integer topicId,

```
....
35.               HttpServletRequest request, HttpServletResponse
response,
....
58.                     return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2396:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2396
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	69	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String topic(@PathVariable Integer id, HttpServletRequest request,

```
....
69.   public String topic(@PathVariable Integer id, HttpServletRequest
request,
....
81.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2397:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2397
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String topic(@PathVariable Integer id, HttpServletRequest request,

```
....
69.   public String topic(@PathVariable Integer id, HttpServletRequest
request,
....
81.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2398:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2398
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String topic(@PathVariable Integer id, HttpServletRequest request,

```
....
69.   public String topic(@PathVariable Integer id, HttpServletRequest
request,
....
81.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2399:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2399
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String topic(@PathVariable Integer id, HttpServletRequest request,

```
....
69.   public String topic(@PathVariable Integer id, HttpServletRequest
request,
....
81.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2400:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2400
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TopicAct.java

方法 public String topic(@PathVariable Integer id, HttpServletRequest request,

```
....
69.   public String topic(@PathVariable Integer id, HttpServletRequest
request,
....
81.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2401:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2401
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	55	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBaidu(HttpServletRequest request,

```
....
55.   public String searchBaidu(HttpServletRequest request,
....
59.         String dizhi=request.getParameter("dizhi");
60.         String name=request.getParameter("name");
....
69.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2402:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2402
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBaidu(HttpServletRequest request,

```
....
55.   public String searchBaidu(HttpServletRequest request,
....
59.         String dizhi=request.getParameter("dizhi");
60.         String name=request.getParameter("name");
....
69.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2403:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2403
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBaidu(HttpServletRequest request,

```
....
55.   public String searchBaidu(HttpServletRequest request,
....
59.         String dizhi=request.getParameter("dizhi");
60.         String name=request.getParameter("name");
....
69.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2404:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2404
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBaidu(HttpServletRequest request,

```
....
55.   public String searchBaidu(HttpServletRequest request,
....
59.         String dizhi=request.getParameter("dizhi");
60.         String name=request.getParameter("name");
....
69.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2405:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2405
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBaidu(HttpServletRequest request,

```
....
55.   public String searchBaidu(HttpServletRequest request,
....
59.         String dizhi=request.getParameter("dizhi");
60.         String name=request.getParameter("name");
....
69.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2406:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2406
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	794	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmledit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
794.        public String matterhtmledit(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
814.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2407:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2407
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	794	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmledit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
794.        public String matterhtmledit(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
814.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2408:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2408
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	794	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmledit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
794.        public String matterhtmledit(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
814.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2409:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2409
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	794	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmledit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
794.        public String matterhtmledit(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
814.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2410:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2410
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	794	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmledit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
794.        public String matterhtmledit(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
814.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2411:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2411
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	849	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmlshow(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
849.        public String matterhtmlshow(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
869.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2412:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2412
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	849	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmlshow(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
849.        public String matterhtmlshow(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
869.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2413:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2413
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	849	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmlshow(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
849.        public String matterhtmlshow(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
869.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2414:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2414
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	849	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmlshow(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
849.        public String matterhtmlshow(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
869.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2415:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2415
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	849	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterhtmlshow(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
849.        public String matterhtmlshow(String sxid, String bsnum,
String redo, HttpServletRequest request,
....
869.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2416:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2416
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	247	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String list(String deptid, String permtype,

```
....
247.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
251.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2417:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2417
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	247	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String list(String deptid, String permtype,

```
....
247.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
251.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2418:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2418
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	247	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String list(String deptid, String permtype,

```
....
247.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
251.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2419:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2419
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	247	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String list(String deptid, String permtype,

```
....
247.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
251.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2420:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2420
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	247	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String list(String deptid, String permtype,

```
....
247.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
251.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2421:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2421
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	283	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.              String name = request.getParameter("selname");
288.              String deptId = request.getParameter("deptId");
....
297.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2422:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2422
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	283	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.              String name = request.getParameter("selname");
288.              String deptId = request.getParameter("deptId");
....
297.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2423:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2423
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	283	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.                String name = request.getParameter("selname");
288.                String deptId = request.getParameter("deptId");
....
297.                      FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2424:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2424
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	283	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.                String name = request.getParameter("selname");
288.                String deptId = request.getParameter("deptId");
....
297.                      FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2425:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2425
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	283	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.                String name = request.getParameter("selname");
288.                String deptId = request.getParameter("deptId");
....
297.                      FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2426:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2426
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	283	36
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
283.        public String lawproduce( HttpServletRequest request,
....
287.              String name = request.getParameter("selname");
....
292.                    name = name.replaceAll("《", "");
293.                    name = name.replaceAll("》", "");
294.                    name = name.trim();
....
304.              List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptId,name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 2427:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2427
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	392	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.              String name = request.getParameter("selname");
....
404.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2428:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2428
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	392	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.              String name = request.getParameter("selname");
....
404.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2429:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2429
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	392	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.              String name = request.getParameter("selname");
....
404.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2430:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2430
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	392	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.              String name = request.getParameter("selname");
....
404.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2431:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2431
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	392	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.              String name = request.getParameter("selname");
....
404.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2432:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2432
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	392	36
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
392.                    Integer pageNo, HttpServletRequest
request,HttpServletResponse response, ModelMap model) {
....
395.                String name = request.getParameter("selname");
....
399.                    name = name.replaceAll("《", "");
400.                    name = name.replaceAll("》", "");
401.                    name = name.trim();
....
411.                List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptid,name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 2433:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2433
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	91	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String zwgkIndex(HttpServletRequest request,

```
....
91.   public String zwgkIndex( HttpServletRequest request,
....
95.         String deptId = request.getParameter("deptId");
....
100.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2434:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2434
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	91	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
91.   public String zwgkIndex( HttpServletRequest request,
....
95.         String deptId = request.getParameter("deptId");
....
100.                  FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2435:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2435
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	91	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String zwgkIndex(HttpServletRequest request,

```
....
91.   public String zwgkIndex( HttpServletRequest request,
....
95.         String deptId = request.getParameter("deptId");
....
100.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2436:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2436
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	91	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
91.   public String zwgkIndex( HttpServletRequest request,
....
95.         String deptId = request.getParameter("deptId");
....
100.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2437:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2437
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	91	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
91.   public String zwgkIndex( HttpServletRequest request,
....
95.         String deptId = request.getParameter("deptId");
....
100.                    FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2438:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2438
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	140	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java
方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
140.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
144.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2439:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2439
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	140	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
140.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
144.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2440:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2440
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	140	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
140.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
144.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2441:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2441
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	140	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
140.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
144.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2442:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2442
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	140	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
140.        public String lawguide(@PathVariable String id,
HttpServletRequest request,
....
144.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2443:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2443
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	219	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
219.        public String download(@PathVariable String id,
HttpServletRequest request,
....
223.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2444:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2444
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	219	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
219.        public String download(@PathVariable String id,
HttpServletRequest request,
....
223.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2445:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2445
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	219	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
219.        public String download(@PathVariable String id,
HttpServletRequest request,
....
223.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2446:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2446
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	219	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
219.        public String download(@PathVariable String id,
HttpServletRequest request,
....
223.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2447:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2447
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	219	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String download(@PathVariable String id, HttpServletRequest request,

```
....
219.        public String download(@PathVariable String id,
HttpServletRequest request,
....
223.                    return FrontUtils.pageNotFound(request,
response, model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2448:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2448
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	49	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
53.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2449:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2449
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	49	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
53.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2450:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2450
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	49	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
53.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2451:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2451
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	49	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
53.                return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2452:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2452
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	49	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java
方法	public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
53.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2453:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2453
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	48	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
52.                return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2454:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2454
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2455:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2455
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2456:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2456
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
52.                return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2457:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2457
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2458:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2458
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	36	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
36.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
40.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2459:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2459
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	36	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
36.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
40.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2460:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2460
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	36	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
36.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
40.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2461:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2461
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
36.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
40.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2462:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2462
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationAct.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
36.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
40.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2463:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2463
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	27	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java
方法	public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
27.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
31.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2464:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2464
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	27	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
27.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
31.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2465:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2465
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	27	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
27.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
31.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2466:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2466
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	27	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java

方法 public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
27.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
31.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2467:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2467
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	27	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebHallIncInfoMationActgr.java
方法	public String lawguide(@PathVariable Integer incid, HttpServletRequest request,

```
....
27.   public String lawguide(@PathVariable Integer incid,
HttpServletRequest request,
....
31.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2468:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2468
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	59	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
63.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2469:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2469
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
63.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2470:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2470
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
63.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2471:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2471
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
63.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2472:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2472
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
63.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2473:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2473
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	54	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java
方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
58.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2474:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2474
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	54	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
58.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2475:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2475
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	54	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
58.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2476:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2476
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	54	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
58.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2477:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2477
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	54	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
58.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2478:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2478
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	48	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2479:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2479
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2480:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2480
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2481:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2481
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2482:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2482
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2483:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2483
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	48	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java
方法	public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2484:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2484
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2485:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2485
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2486:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2486
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.                 return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2487:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2487
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
52.               return FrontUtils.pageNotFound(request, response,
model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String pageNotFound(HttpServletRequest request,

```
....
211.        public static String pageNotFound(HttpServletRequest
request,
....
215.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2488:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2488
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	77	37
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java
方法 public String detail(@PathVariable Integer id, HttpServletRequest request,

```
....
77.   public String detail(@PathVariable Integer id, HttpServletRequest
request,
....
81.               return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2489:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2489
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	77	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String detail(@PathVariable Integer id, HttpServletRequest request,

```
....
77.   public String detail(@PathVariable Integer id, HttpServletRequest
request,
....
81.               return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2490:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2490
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	77	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String detail(@PathVariable Integer id, HttpServletRequest request,

```
....
77.   public String detail(@PathVariable Integer id, HttpServletRequest
request,
....
81.                 return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2491:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2491
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	77	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String detail(@PathVariable Integer id, HttpServletRequest request,

```
....
77.   public String detail(@PathVariable Integer id, HttpServletRequest
request,
....
81.                 return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2492:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2492
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	77	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String detail(@PathVariable Integer id, HttpServletRequest request,

```
....
77.   public String detail(@PathVariable Integer id, HttpServletRequest
request,
....
81.                 return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2493:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2493
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	205	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
205.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
212.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2494:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2494
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
205.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
212.              return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2495:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2495
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
205.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
212.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2496:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2496
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
205.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
212.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2497:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2497
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitem(@PathVariable String id, HttpServletRequest request,

```
....
205.        public String permissionitem(@PathVariable String id,
HttpServletRequest request,
....
212.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2498:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2498
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	230	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
230.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
235.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2499:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2499
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	230	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
230.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
235.              return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2500:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2500
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	230	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
230.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
235.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2501:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2501
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	230	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
230.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
235.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2502:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2502
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	230	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
230.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
235.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2503:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2503
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	248	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitemGet(HttpServletRequest request,

```
....
248.        public String selpermissionitemGet(HttpServletRequest
request,
....
251.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
253.                String name  = request.getParameter("selname");
....
255.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2504:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2504
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	248	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitemGet(HttpServletRequest request,

```
....
248.        public String selpermissionitemGet(HttpServletRequest
request,
....
251.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
253.              String name  = request.getParameter("selname");
....
255.              return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2505:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2505
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	248	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitemGet(HttpServletRequest request,

```
....
248.        public String selpermissionitemGet(HttpServletRequest
request,
....
251.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
253.                String name  = request.getParameter("selname");
....
255.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2506:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2506
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	248	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitemGet(HttpServletRequest request,

```
....
248.        public String selpermissionitemGet(HttpServletRequest
request,
....
251.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
253.                String name  = request.getParameter("selname");
....
255.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2507:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2507
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	248	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitemGet(HttpServletRequest request,

```
....
248.        public String selpermissionitemGet(HttpServletRequest
request,
....
251.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
253.                String name  = request.getParameter("selname");
....
255.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2508:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2508
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	279	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
279.        public String selpermissionitem(HttpServletRequest request,
....
282.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
284.                String name  = request.getParameter("selname");
....
286.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2509:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2509
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	279	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
279.        public String selpermissionitem(HttpServletRequest request,
....
282.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
284.              String name  = request.getParameter("selname");
....
286.              return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2510:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2510
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	279	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
279.        public String selpermissionitem(HttpServletRequest request,
....
282.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
284.                String name  = request.getParameter("selname");
....
286.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2511:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2511
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	279	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
279.        public String selpermissionitem(HttpServletRequest request,
....
282.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
284.                String name  = request.getParameter("selname");
....
286.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2512:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2512
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	279	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
279.        public String selpermissionitem(HttpServletRequest request,
....
282.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
284.                String name  = request.getParameter("selname");
....
286.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2513:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2513
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	347	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitemsxinfo(@PathVariable String id, HttpServletRequest request,

```
....
347.        public String permissionitemsxinfo(@PathVariable String id,
HttpServletRequest request,
....
352.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2514:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2514
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	347	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitemsxinfo(@PathVariable String id, HttpServletRequest request,

```
....
347.        public String permissionitemsxinfo(@PathVariable String id,
HttpServletRequest request,
....
352.              UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.              return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2515:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2515
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	347	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitemsxinfo(@PathVariable String id, HttpServletRequest request,

```
....
347.        public String permissionitemsxinfo(@PathVariable String id,
HttpServletRequest request,
....
352.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2516:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2516
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	347	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitemsxinfo(@PathVariable String id, HttpServletRequest request,

```
....
347.        public String permissionitemsxinfo(@PathVariable String id,
HttpServletRequest request,
....
352.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2517:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2517
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	347	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permissionitemsxinfo(@PathVariable String id, HttpServletRequest request,

```
....
347.        public String permissionitemsxinfo(@PathVariable String id,
HttpServletRequest request,
....
352.                UnifiedUser user =(UnifiedUser)
request.getSession().getAttribute("sessionuser");
....
354.                return FrontUtils.showError(request, response, model,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2518:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2518
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	149	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
149.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
153.                String type = request.getParameter("type");
....
156.                        return FrontUtils.showError(request, response,
model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2519:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2519
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	149	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
149.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
153.              String type = request.getParameter("type");
....
156.                    return FrontUtils.showError(request, response,
model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2520:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2520
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	149	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
149.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
153.                String type = request.getParameter("type");
....
156.                      return FrontUtils.showError(request, response,
model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2521:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2521
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	149	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
149.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
153.                String type = request.getParameter("type");
....
156.                        return FrontUtils.showError(request, response,
model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2522:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2522
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	149	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String refercomplain(@PathVariable String id, HttpServletRequest request,

```
....
149.        public String refercomplain(@PathVariable String id,
HttpServletRequest request,
....
153.                String type = request.getParameter("type");
....
156.                      return FrontUtils.showError(request, response,
model, null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2523:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2523
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	79	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordSubmit(String username, String email,

```
....
79.                 String captcha_find, HttpServletRequest request,
....
82.         captcha_find = request.getParameter("captcha_find");
....
90.                 return FrontUtils.showError(request, response, model,
errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2524:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2524
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	79	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordSubmit(String username, String email,

```
....
79.               String captcha_find, HttpServletRequest request,
....
82.         captcha_find = request.getParameter("captcha_find");
....
90.               return FrontUtils.showError(request, response, model,
errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2525:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2525
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	79	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordSubmit(String username, String email,

```
....
79.                 String captcha_find, HttpServletRequest request,
....
82.         captcha_find = request.getParameter("captcha_find");
....
90.                 return FrontUtils.showError(request, response, model,
errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2526:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2526
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	79	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordSubmit(String username, String email,

```
....
79.                 String captcha_find, HttpServletRequest request,
....
82.         captcha_find = request.getParameter("captcha_find");
....
90.                 return FrontUtils.showError(request, response, model,
errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2527:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2527
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	79	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordSubmit(String username, String email,

```
....
79.                 String captcha_find, HttpServletRequest request,
....
82.         captcha_find = request.getParameter("captcha_find");
....
90.                 return FrontUtils.showError(request, response, model,
errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2528:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2528
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	129	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String passwordReset(Integer uid, String key,

```
....
129.                    HttpServletRequest request, HttpServletResponse
response,
....
134.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2529:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2529
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String passwordReset(Integer uid, String key,

```
....
129.                    HttpServletRequest request, HttpServletResponse
response,
....
134.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2530:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2530
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String passwordReset(Integer uid, String key,

```
....
129.                    HttpServletRequest request, HttpServletResponse
response,
....
134.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2531:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2531
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String passwordReset(Integer uid, String key,

```
....
129.                    HttpServletRequest request, HttpServletResponse
response,
....
134.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2532:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2532
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String passwordReset(Integer uid, String key,

```
....
129.                    HttpServletRequest request, HttpServletResponse
response,
....
134.                    return FrontUtils.showError(request, response,
model, errors);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showError(HttpServletRequest request,

```
....
246.        public static String showError(HttpServletRequest request,
....
250.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2533:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2533
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	736	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String jiezhenfuwu(HttpServletRequest request, ModelMap model) {

```
....
736.        public String jiezhenfuwu(HttpServletRequest request,
ModelMap model) {
....
738.                String region = request.getParameter("service");
....
751.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2534:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2534
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	736	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String jiezhenfuwu(HttpServletRequest request, ModelMap model) {

```
....
736.        public String jiezhenfuwu(HttpServletRequest request,
ModelMap model) {
....
738.              String region = request.getParameter("service");
....
751.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2535:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2535
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	736	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String jiezhenfuwu(HttpServletRequest request, ModelMap model) {

```
....
736.        public String jiezhenfuwu(HttpServletRequest request,
ModelMap model) {
....
738.              String region = request.getParameter("service");
....
751.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2536:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2536
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	736	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java
方法	public String jiezhenfuwu(HttpServletRequest request, ModelMap model) {

```
....
736.        public String jiezhenfuwu(HttpServletRequest request,
ModelMap model) {
....
738.              String region = request.getParameter("service");
....
751.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2537:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2537
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	736	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/DynamicPageAct.java

方法 public String jiezhenfuwu(HttpServletRequest request, ModelMap model) {

```
....
736.        public String jiezhenfuwu(HttpServletRequest request,
ModelMap model) {
....
738.                String region = request.getParameter("service");
....
751.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2538:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2538
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	49	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
49.   public String search(String linkname, HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2539:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2539
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	49	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
49.   public String search(String linkname, HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2540:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2540
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	49	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java
方法	public String search(String linkname, HttpServletRequest request,

```
....
49.   public String search(String linkname, HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2541:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2541
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	49	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
49.   public String search(String linkname, HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2542:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2542
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	49	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
49.   public String search(String linkname, HttpServletRequest request,
....
54.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2543:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2543
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	55	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String index(Integer ctgId, HttpServletRequest request,

```
....
55.   public String index(Integer ctgId, HttpServletRequest request,
....
58.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2544:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2544
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String index(Integer ctgId, HttpServletRequest request,

```
....
55.   public String index(Integer ctgId, HttpServletRequest request,
....
58.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2545:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2545
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java
方法	public String index(Integer ctgId, HttpServletRequest request,

```
....
55.   public String index(Integer ctgId, HttpServletRequest request,
....
58.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2546:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2546
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String index(Integer ctgId, HttpServletRequest request,

```
....
55.   public String index(Integer ctgId, HttpServletRequest request,
....
58.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2547:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2547
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/GuestbookAct.java

方法 public String index(Integer ctgId, HttpServletRequest request,

```
....
55.   public String index(Integer ctgId, HttpServletRequest request,
....
58.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2548:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2548
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	71	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
71.   public String toHdjl( HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2549:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2549
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	71	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
71.   public String toHdjl( HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2550:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2550
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	71	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String toHdjl(HttpServletRequest request,

```
....
71.   public String toHdjl( HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2551:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2551
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	71	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
71.   public String toHdjl( HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2552:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2552
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	71	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toHdjl(HttpServletRequest request,

```
....
71.   public String toHdjl( HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2553:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2553
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	80	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toCJDH(HttpServletRequest request,

```
....
80.   public String toCJDH( HttpServletRequest request,
....
83.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2554:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2554
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	80	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toCJDH(HttpServletRequest request,

```
....
80.   public String toCJDH( HttpServletRequest request,
....
83.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2555:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2555
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	80	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String toCJDH(HttpServletRequest request,

```
....
80.   public String toCJDH( HttpServletRequest request,
....
83.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2556:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2556
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	80	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toCJDH(HttpServletRequest request,

```
....
80.   public String toCJDH( HttpServletRequest request,
....
83.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2557:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2557
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	80	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toCJDH(HttpServletRequest request,

```
....
80.   public String toCJDH( HttpServletRequest request,
....
83.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2558:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2558
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	98	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
98.   public String toAddZx(String sxid,HttpServletRequest request,
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2559:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2559
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	98	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
98.   public String toAddZx(String sxid,HttpServletRequest request,
....
119.            FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2560:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2560
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	98	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
98.   public String toAddZx(String sxid,HttpServletRequest request,
....
119.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2561:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2561
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	98	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
98.   public String toAddZx(String sxid,HttpServletRequest request,
....
119.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2562:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2562
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	98	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
98.   public String toAddZx(String sxid,HttpServletRequest request,
....
119.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2563:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2563
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	160	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxList(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
160.        public String zxList(String queryTitle,Integer
pageNo,HttpServletRequest request,
....
163.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2564:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2564
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	160	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxList(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
160.        public String zxList(String queryTitle,Integer
pageNo,HttpServletRequest request,
....
163.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2565:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2565
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	160	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxList(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
160.        public String zxList(String queryTitle,Integer
pageNo,HttpServletRequest request,
....
163.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2566:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2566
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	160	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String zxList(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
160.        public String zxList(String queryTitle,Integer
pageNo,HttpServletRequest request,
....
163.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2567:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2567
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	160	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxList(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
160.        public String zxList(String queryTitle,Integer
pageNo,HttpServletRequest request,
....
163.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2568:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2568
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	178	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
178.        public String show(Integer id,HttpServletRequest request,
....
181.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2569:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2569
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	178	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
178.        public String show(Integer id,HttpServletRequest request,
....
181.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2570:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2570
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	178	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String show(Integer id,HttpServletRequest request,

```
....
178.        public String show(Integer id,HttpServletRequest request,
....
181.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2571:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2571
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	178	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
178.        public String show(Integer id,HttpServletRequest request,
....
181.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2572:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2572
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	178	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String show(Integer id,HttpServletRequest request,

```
....
178.        public String show(Integer id,HttpServletRequest request,
....
181.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2573:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2573
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	190	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxlist(String queryTitle, String deptId,

```
....
190.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
192.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2574:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2574
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	190	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxlist(String queryTitle, String deptId,

```
....
190.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
192.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2575:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2575
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	190	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxlist(String queryTitle, String deptId,

```
....
190.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
192.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2576:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2576
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	190	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String zxlist(String queryTitle, String deptId,

```
....
190.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
192.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2577:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2577
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	190	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String zxlist(String queryTitle, String deptId,

```
....
190.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
192.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2578:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2578
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	205	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTs(String deptid,HttpServletRequest request,

```
....
205.        public String toAddTs(String deptid,HttpServletRequest
request,
....
215.                    Object areaId =
request.getSession().getAttribute("areaId");
....
217.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2579:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2579
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTs(String deptid,HttpServletRequest request,

```
....
205.        public String toAddTs(String deptid,HttpServletRequest
request,
....
223.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2580:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2580
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTs(String deptid,HttpServletRequest request,

```
....
205.        public String toAddTs(String deptid,HttpServletRequest
request,
....
223.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2581:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2581
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTs(String deptid,HttpServletRequest request,

```
....
205.        public String toAddTs(String deptid,HttpServletRequest
request,
....
223.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2582:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2582
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTs(String deptid,HttpServletRequest request,

```
....
205.        public String toAddTs(String deptid,HttpServletRequest
request,
....
223.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2583:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2583
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	229	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAndroid(String deptid,HttpServletRequest request,

```
....
229.        public String toAndroid(String deptid,HttpServletRequest
request,
....
234.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2584:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2584
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	229	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAndroid(String deptid,HttpServletRequest request,

```
....
229.        public String toAndroid(String deptid,HttpServletRequest
request,
....
234.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2585:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2585
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	229	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAndroid(String deptid,HttpServletRequest request,

```
....
229.        public String toAndroid(String deptid,HttpServletRequest
request,
....
234.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2586:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2586
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	229	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String toAndroid(String deptid,HttpServletRequest request,

```
....
229.        public String toAndroid(String deptid,HttpServletRequest
request,
....
234.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2587:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2587
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	229	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAndroid(String deptid,HttpServletRequest request,

```
....
229.        public String toAndroid(String deptid,HttpServletRequest
request,
....
234.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2588:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2588
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	241	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveTs(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
241.                    String content,String nextUrl, String
wsts_captcha,HttpServletRequest request,
....
249.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2589:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2589
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	241	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveTs(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
241.                    String content,String nextUrl, String
wsts_captcha,HttpServletRequest request,
....
249.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2590:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2590
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	241	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveTs(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
241.                    String content,String nextUrl, String
wsts_captcha,HttpServletRequest request,
....
249.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2591:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2591
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	241	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String saveTs(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
241.                    String content,String nextUrl, String
wsts_captcha,HttpServletRequest request,
....
249.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2592:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2592
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	241	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveTs(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
241.                    String content,String nextUrl, String
wsts_captcha,HttpServletRequest request,
....
249.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2593:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2593
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	126	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveZx(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
126.                    String content,String nextUrl, String
wszx_captcha,HttpServletRequest request,
....
157.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2594:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2594
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	126	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveZx(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
126.                    String content,String nextUrl, String
wszx_captcha,HttpServletRequest request,
....
157.              return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2595:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2595
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	126	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveZx(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
126.                    String content,String nextUrl, String
wszx_captcha,HttpServletRequest request,
....
157.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2596:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2596
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	126	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveZx(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
126.                    String content,String nextUrl, String
wszx_captcha,HttpServletRequest request,
....
157.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2597:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2597
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	126	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String saveZx(TWebhallReferComplain rc, String maintitle, String departmentid,

```
....
126.                    String content,String nextUrl, String
wszx_captcha,HttpServletRequest request,
....
157.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2598:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2598
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	205	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String addopinionrecord(String opinion_title,String opinion_username,

```
....
205.                    HttpServletRequest request,HttpServletResponse
response, ModelMap model) {
....
224.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2599:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2599
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String addopinionrecord(String opinion_title,String opinion_username,

```
....
205.                    HttpServletRequest request,HttpServletResponse
response, ModelMap model) {
....
224.              return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2600:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2600
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	205	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String addopinionrecord(String opinion_title,String opinion_username,

```
....
205.                    HttpServletRequest request,HttpServletResponse
response, ModelMap model) {
....
224.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2601:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2601
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String addopinionrecord(String opinion_title,String opinion_username,

```
....
205.                    HttpServletRequest request,HttpServletResponse
response, ModelMap model) {
....
224.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2602:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2602
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	205	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String addopinionrecord(String opinion_title,String opinion_username,

```
....
205.                    HttpServletRequest request,HttpServletResponse
response, ModelMap model) {
....
224.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2603:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2603
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	82	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String saveSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
82.   public String saveSync(String sync_id,String sync_cron,String
nextUrl,HttpServletRequest request,
....
96.         return FrontUtils.showSuccess(request, model, nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2604:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2604
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	82	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String saveSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
82.   public String saveSync(String sync_id,String sync_cron,String
nextUrl,HttpServletRequest request,
....
96.         return FrontUtils.showSuccess(request, model, nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2605:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2605
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	82	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String saveSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
82.   public String saveSync(String sync_id,String sync_cron,String
nextUrl,HttpServletRequest request,
....
96.         return FrontUtils.showSuccess(request, model, nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2606:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2606
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	82	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String saveSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
82.   public String saveSync(String sync_id,String sync_cron,String
nextUrl,HttpServletRequest request,
....
96.         return FrontUtils.showSuccess(request, model, nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2607:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2607
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	82	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String saveSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
82.   public String saveSync(String sync_id,String sync_cron,String
nextUrl,HttpServletRequest request,
....
96.         return FrontUtils.showSuccess(request, model, nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2608:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2608
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	115	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String eidtSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
115.        public String eidtSync(String sync_id,String
sync_cron,String nextUrl,HttpServletRequest request,
....
129.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2609:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2609
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	115	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String eidtSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
115.        public String eidtSync(String sync_id,String
sync_cron,String nextUrl,HttpServletRequest request,
....
129.              return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.              frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2610:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2610
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	115	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String eidtSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
115.        public String eidtSync(String sync_id,String
sync_cron,String nextUrl,HttpServletRequest request,
....
129.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2611:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2611
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	115	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String eidtSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
115.        public String eidtSync(String sync_id,String
sync_cron,String nextUrl,HttpServletRequest request,
....
129.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2612:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2612
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	115	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String eidtSync(String sync_id,String sync_cron,String nextUrl,HttpServletRequest request,

```
....
115.        public String eidtSync(String sync_id,String
sync_cron,String nextUrl,HttpServletRequest request,
....
129.                return FrontUtils.showSuccess(request, model,
nextUrl);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String showSuccess(HttpServletRequest request,

```
....
227.        public static String showSuccess(HttpServletRequest request,
....
230.                frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2613:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2613
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	296	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
296.        public String toAddZxTwo(String sxid,HttpServletRequest
request,
....
309.                    String areaId = request.getParameter("areaId");
....
311.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2614:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2614
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	296	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
296.        public String toAddZxTwo(String sxid,HttpServletRequest
request,
....
314.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2615:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2615
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	296	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
296.        public String toAddZxTwo(String sxid,HttpServletRequest
request,
....
314.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2616:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2616
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	296	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
296.        public String toAddZxTwo(String sxid,HttpServletRequest
request,
....
314.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2617:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2617
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	296	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
296.        public String toAddZxTwo(String sxid,HttpServletRequest
request,
....
314.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2618:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2618
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	69	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String sortsearch(String ctgid, HttpServletRequest request,

```
....
69.   public String sortsearch(String ctgid, HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2619:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2619
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String sortsearch(String ctgid, HttpServletRequest request,

```
....
69.   public String sortsearch(String ctgid, HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2620:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2620
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	69	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java
方法	public String sortsearch(String ctgid, HttpServletRequest request,

```
....
69.   public String sortsearch(String ctgid, HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2621:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2621
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String sortsearch(String ctgid, HttpServletRequest request,

```
....
69.   public String sortsearch(String ctgid, HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2622:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2622
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	69	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/FriendlinkAct.java

方法 public String sortsearch(String ctgid, HttpServletRequest request,

```
....
69.   public String sortsearch(String ctgid, HttpServletRequest request,
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2623:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2623
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	320	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
320.        public String toAddTsTwo(String deptid,HttpServletRequest
request,
....
330.                    String areaId = request.getParameter("areaId");
....
332.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2624:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2624
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	320	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
320.        public String toAddTsTwo(String deptid,HttpServletRequest
request,
....
335.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2625:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2625
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	320	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
320.        public String toAddTsTwo(String deptid,HttpServletRequest
request,
....
335.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2626:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2626
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	320	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
320.        public String toAddTsTwo(String deptid,HttpServletRequest
request,
....
335.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2627:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2627
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	320	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
320.        public String toAddTsTwo(String deptid,HttpServletRequest
request,
....
335.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2628:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2628
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	340	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String jianshezhong(HttpServletRequest request, ModelMap model) {

```
....
340.        public String jianshezhong(HttpServletRequest request,
ModelMap model) {
....
343.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2629:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2629
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	340	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String jianshezhong(HttpServletRequest request, ModelMap model) {

```
....
340.        public String jianshezhong(HttpServletRequest request,
ModelMap model) {
....
343.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2630:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2630
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	340	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String jianshezhong(HttpServletRequest request, ModelMap model) {

```
....
340.        public String jianshezhong(HttpServletRequest request,
ModelMap model) {
....
343.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2631:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2631
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	340	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String jianshezhong(HttpServletRequest request, ModelMap model) {

```
....
340.        public String jianshezhong(HttpServletRequest request,
ModelMap model) {
....
343.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2632:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2632
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	340	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String jianshezhong(HttpServletRequest request, ModelMap model) {

```
....
340.        public String jianshezhong(HttpServletRequest request,
ModelMap model) {
....
343.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2633:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2633
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	87	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String preCounsel1(HttpServletRequest request, ModelMap model) {

```
....
87.   public String preCounsel1(HttpServletRequest request, ModelMap
model) {
....
89.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2634:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2634
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	87	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String preCounsel1(HttpServletRequest request, ModelMap model) {

```
....
87.   public String preCounsel1(HttpServletRequest request, ModelMap
model) {
....
89.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2635:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2635
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	87	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String preCounsel1(HttpServletRequest request, ModelMap model) {

```
....
87.   public String preCounsel1(HttpServletRequest request, ModelMap
model) {
....
89.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2636:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2636
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	87	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java
方法	public String preCounsel1(HttpServletRequest request, ModelMap model) {

```
....
87.   public String preCounsel1(HttpServletRequest request, ModelMap
model) {
....
89.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2637:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2637
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	87	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public String preCounsel1(HttpServletRequest request, ModelMap model) {

```
....
87.   public String preCounsel1(HttpServletRequest request, ModelMap
model) {
....
89.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2638:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2638
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	89	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String dongmandating(HttpServletRequest request,

```
....
89.   public String dongmandating( HttpServletRequest request,
....
92.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2639:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2639
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	89	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String dongmandating(HttpServletRequest request,

```
....
89.   public String dongmandating( HttpServletRequest request,
....
92.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2640:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2640
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	89	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String dongmandating(HttpServletRequest request,

```
....
89.   public String dongmandating( HttpServletRequest request,
....
92.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2641:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2641
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	89	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String dongmandating(HttpServletRequest request,

```
....
89.   public String dongmandating( HttpServletRequest request,
....
92.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2642:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2642
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	89	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String dongmandating(HttpServletRequest request,

```
....
89.   public String dongmandating( HttpServletRequest request,
....
92.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2643:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2643
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	138	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
142.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2644:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2644
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	138	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
142.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2645:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2645
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	138	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
142.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2646:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2646
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
142.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2647:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2647
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String dept(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
138.        public String dept(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
142.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2648:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2648
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	195	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,

```
....
195.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
197.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2649:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2649
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	195	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,

```
....
195.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
197.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2650:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2650
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	195	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,

```
....
195.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
197.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2651:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2651
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	195	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String tableList(String areaId,

```
....
195.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
197.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2652:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2652
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	195	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,

```
....
195.                    Integer pageNo, HttpServletRequest request,
ModelMap model) {
....
197.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2653:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2653
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	283	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String showTs(Integer id,HttpServletRequest request,

```
....
283.        public String showTs(Integer id,HttpServletRequest request,
....
287.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2654:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2654
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	283	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String showTs(Integer id,HttpServletRequest request,

```
....
283.        public String showTs(Integer id,HttpServletRequest request,
....
287.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2655:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2655
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	283	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法	public String showTs(Integer id,HttpServletRequest request,

```
....
283.        public String showTs(Integer id,HttpServletRequest request,
....
287.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2656:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2656
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	283	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String showTs(Integer id,HttpServletRequest request,

```
....
283.        public String showTs(Integer id,HttpServletRequest request,
....
287.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2657:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2657
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	283	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String showTs(Integer id,HttpServletRequest request,

```
....
283.        public String showTs(Integer id,HttpServletRequest request,
....
287.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2658:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2658
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	182	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
186.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2659:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2659
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	182	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
186.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2660:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2660
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	182	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
186.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2661:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2661
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
186.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2662:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2662
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	182	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
182.        public String tableList(String areaId,HttpServletRequest
request, HttpServletResponse response,
....
186.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2663:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2663
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	698	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String schedule(HttpServletRequest request, HttpServletResponse response,

```
....
698.        public String schedule(HttpServletRequest request,
HttpServletResponse response,
....
701.                String id = request.getParameter("bsnum");
702.                String first = request.getParameter("first");
703.                String captcha =
request.getParameter("schedulecaptcha");
704.                String member = request.getParameter("member") == null
? "" : request.getParameter("member");
....
719.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2664:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2664
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	698	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String schedule(HttpServletRequest request, HttpServletResponse response,

```
....
698.        public String schedule(HttpServletRequest request,
HttpServletResponse response,
....
701.                String id = request.getParameter("bsnum");
702.                String first = request.getParameter("first");
703.                String captcha =
request.getParameter("schedulecaptcha");
704.                String member = request.getParameter("member") == null
? "" : request.getParameter("member");
....
719.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2665:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2665
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/cms/action/front/LawGuideAct.java	cms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	698	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String schedule(HttpServletRequest request, HttpServletResponse response,

```
....
698.        public String schedule(HttpServletRequest request,
HttpServletResponse response,
....
701.                String id = request.getParameter("bsnum");
702.                String first = request.getParameter("first");
703.                String captcha =
request.getParameter("schedulecaptcha");
704.                String member = request.getParameter("member") == null
? "" : request.getParameter("member");
....
719.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2666:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2666
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	698	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法 public String schedule(HttpServletRequest request, HttpServletResponse response,

```
....
698.        public String schedule(HttpServletRequest request,
HttpServletResponse response,
....
701.                String id = request.getParameter("bsnum");
702.                String first = request.getParameter("first");
703.                String captcha =
request.getParameter("schedulecaptcha");
704.                String member = request.getParameter("member") == null
? "" : request.getParameter("member");
....
719.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2667:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2667
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	698	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String schedule(HttpServletRequest request, HttpServletResponse response,

```
....
698.        public String schedule(HttpServletRequest request,
HttpServletResponse response,
....
701.                String id = request.getParameter("bsnum");
702.                String first = request.getParameter("first");
703.                String captcha =
request.getParameter("schedulecaptcha");
704.                String member = request.getParameter("member") == null
? "" : request.getParameter("member");
....
719.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2668:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2668
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	742	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String doSearch(HttpServletRequest request, HttpServletResponse response,

```
....
742.        public String doSearch(HttpServletRequest request,
HttpServletResponse response,
....
745.                String bid = request.getParameter("bid");
746.                String bsrname = request.getParameter("bsrxm");
....
748.                String bsinfo_captcha =
request.getParameter("searchcaptcha");
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2669:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2669
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	742	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearch(HttpServletRequest request, HttpServletResponse response,

```
....
742.        public String doSearch(HttpServletRequest request,
HttpServletResponse response,
....
745.              String bid = request.getParameter("bid");
746.              String bsrname = request.getParameter("bsrxm");
....
748.              String bsinfo_captcha =
request.getParameter("searchcaptcha");
....
754.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2670:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2670
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	742	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearch(HttpServletRequest request, HttpServletResponse response,

```
....
742.        public String doSearch(HttpServletRequest request,
HttpServletResponse response,
....
745.                String bid = request.getParameter("bid");
746.                String bsrname = request.getParameter("bsrxm");
....
748.                String bsinfo_captcha =
request.getParameter("searchcaptcha");
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2671:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2671
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	742	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearch(HttpServletRequest request, HttpServletResponse response,

```
....
742.        public String doSearch(HttpServletRequest request,
HttpServletResponse response,
....
745.                String bid = request.getParameter("bid");
746.                String bsrname = request.getParameter("bsrxm");
....
748.                String bsinfo_captcha =
request.getParameter("searchcaptcha");
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2672:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2672
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	742	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearch(HttpServletRequest request, HttpServletResponse response,

```
....
742.        public String doSearch(HttpServletRequest request,
HttpServletResponse response,
....
745.                String bid = request.getParameter("bid");
746.                String bsrname = request.getParameter("bsrxm");
....
748.                String bsinfo_captcha =
request.getParameter("searchcaptcha");
....
754.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2673:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2673
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	761	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearchBidCode(HttpServletRequest request, HttpServletResponse response,

```
....
761.        public String doSearchBidCode(HttpServletRequest request,
HttpServletResponse response,
....
764.                String bid = request.getParameter("bid");
....
767.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2674:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2674
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	761	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearchBidCode(HttpServletRequest request, HttpServletResponse response,

```
....
761.        public String doSearchBidCode(HttpServletRequest request,
HttpServletResponse response,
....
764.                String bid = request.getParameter("bid");
....
767.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2675:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2675
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	761	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearchBidCode(HttpServletRequest request, HttpServletResponse response,

```
....
761.        public String doSearchBidCode(HttpServletRequest request,
HttpServletResponse response,
....
764.                String bid = request.getParameter("bid");
....
767.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2676:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2676
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	761	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String doSearchBidCode(HttpServletRequest request, HttpServletResponse response,

```
....
761.        public String doSearchBidCode(HttpServletRequest request,
HttpServletResponse response,
....
764.                String bid = request.getParameter("bid");
....
767.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2677:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2677
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	761	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String doSearchBidCode(HttpServletRequest request, HttpServletResponse response,

```
....
761.        public String doSearchBidCode(HttpServletRequest request,
HttpServletResponse response,
....
764.                String bid = request.getParameter("bid");
....
767.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2678:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2678
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	774	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2679:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2679
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	774	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2680:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2680
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	774	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2681:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2681
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	774	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2682:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2682
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	774	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2683:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2683
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	812	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfoGet(HttpServletRequest request, HttpServletResponse response,

```
....
812.        public String businessinfoGet(HttpServletRequest request,
HttpServletResponse response,
....
814.                return businessinfo(request,response,model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2684:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2684
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	812	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfoGet(HttpServletRequest request, HttpServletResponse response,

```
....
812.        public String businessinfoGet(HttpServletRequest request,
HttpServletResponse response,
....
814.              return businessinfo(request,response,model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2685:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2685
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	812	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfoGet(HttpServletRequest request, HttpServletResponse response,

```
....
812.        public String businessinfoGet(HttpServletRequest request,
HttpServletResponse response,
....
814.              return businessinfo(request,response,model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2686:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2686
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	812	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfoGet(HttpServletRequest request, HttpServletResponse response,

```
....
812.        public String businessinfoGet(HttpServletRequest request,
HttpServletResponse response,
....
814.              return businessinfo(request,response,model);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2687:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2687
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	812	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String businessinfoGet(HttpServletRequest request, HttpServletResponse response,

```
....
812.        public String businessinfoGet(HttpServletRequest request,
HttpServletResponse response,
....
814.                return businessinfo(request,response,model);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String businessinfo(HttpServletRequest request, HttpServletResponse response,

```
....
774.        public String businessinfo(HttpServletRequest request,
HttpServletResponse response,
....
777.                String id = request.getParameter("bid");
....
779.                String bsinfo_captcha =
request.getParameter("bsinfo_captcha");
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2688:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2688
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	885	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
885.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
888.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java
方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                        Object areaId =
request.getSession().getAttribute("areaId");
....
113.                        List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2689:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2689
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	885	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
885.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
888.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2690:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2690
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	885	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
885.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
888.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2691:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2691
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	885	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
885.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
888.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2692:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2692
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	885	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
885.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
888.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2693:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2693
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	630	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String downloadFile(HttpServletRequest request, HttpServletResponse response,

```
....
630.        public String downloadFile(HttpServletRequest request,
HttpServletResponse response,
....
633.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2694:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2694
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	630	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String downloadFile(HttpServletRequest request, HttpServletResponse response,

```
....
630.        public String downloadFile(HttpServletRequest request,
HttpServletResponse response,
....
633.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2695:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2695
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	630	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String downloadFile(HttpServletRequest request, HttpServletResponse response,

```
....
630.        public String downloadFile(HttpServletRequest request,
HttpServletResponse response,
....
633.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2696:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2696
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	630	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String downloadFile(HttpServletRequest request, HttpServletResponse response,

```
....
630.        public String downloadFile(HttpServletRequest request,
HttpServletResponse response,
....
633.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2697:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2697
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	630	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String downloadFile(HttpServletRequest request, HttpServletResponse response,

```
....
630.        public String downloadFile(HttpServletRequest request,
HttpServletResponse response,
....
633.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2698:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2698
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1089	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionZhenJieitem(HttpServletRequest request,

```
....
1089.       public String selpermissionZhenJieitem(HttpServletRequest
request,
....
1092.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2699:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2699
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1089	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionZhenJieitem(HttpServletRequest request,

```
....
1089.       public String selpermissionZhenJieitem(HttpServletRequest
request,
....
1092.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2700:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2700
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1089	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionZhenJieitem(HttpServletRequest request,

```
....
1089.       public String selpermissionZhenJieitem(HttpServletRequest
request,
....
1092.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2701:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2701
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1089	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String selpermissionZhenJieitem(HttpServletRequest request,

```
....
1089.       public String selpermissionZhenJieitem(HttpServletRequest
request,
....
1092.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2702:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2702
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1089	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String selpermissionZhenJieitem(HttpServletRequest request,

```
....
1089.       public String selpermissionZhenJieitem(HttpServletRequest
request,
....
1092.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2703:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2703
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	731	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String preSearch(HttpServletRequest request, HttpServletResponse response,

```
....
731.        public String preSearch(HttpServletRequest request,
HttpServletResponse response,
....
734.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2704:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2704
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	731	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String preSearch(HttpServletRequest request, HttpServletResponse response,

```
....
731.        public String preSearch(HttpServletRequest request,
HttpServletResponse response,
....
734.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2705:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2705
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	731	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String preSearch(HttpServletRequest request, HttpServletResponse response,

```
....
731.        public String preSearch(HttpServletRequest request,
HttpServletResponse response,
....
734.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2706:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2706
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	731	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java
方法	public String preSearch(HttpServletRequest request, HttpServletResponse response,

```
....
731.        public String preSearch(HttpServletRequest request,
HttpServletResponse response,
....
734.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2707:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2707
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	731	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String preSearch(HttpServletRequest request, HttpServletResponse response,

```
....
731.        public String preSearch(HttpServletRequest request,
HttpServletResponse response,
....
734.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2708:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2708
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	57	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public void submit(String opinion_title,String opinion_username,

```
....
57.                 HttpServletRequest request,
....
63.                 if(!captcha.validate(request, "opinionRecord_captcha",
model)){
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public boolean validate(HttpServletRequest request,String captcha_name,ModelMap model){

```
....
91.   public boolean validate(HttpServletRequest request,String
captcha_name,ModelMap model){
92.         String captcha = request.getParameter(captcha_name);
....
118.                    FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2709:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2709
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	57	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public void submit(String opinion_title,String opinion_username,

```
....
57.               HttpServletRequest request,
....
63.               if(!captcha.validate(request, "opinionRecord_captcha",
model)){
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public boolean validate(HttpServletRequest request,String captcha_name,ModelMap model){

```
....
91.   public boolean validate(HttpServletRequest request,String
captcha_name,ModelMap model){
92.         String captcha = request.getParameter(captcha_name);
....
118.                    FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2710:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2710
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	57	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public void submit(String opinion_title,String opinion_username,

```
....
57.                 HttpServletRequest request,
....
63.                 if(!captcha.validate(request, "opinionRecord_captcha",
model)){
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public boolean validate(HttpServletRequest request,String captcha_name,ModelMap model){

```
....
91.   public boolean validate(HttpServletRequest request,String
captcha_name,ModelMap model){
92.         String captcha = request.getParameter(captcha_name);
....
118.                    FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2711:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2711
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	57	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public void submit(String opinion_title,String opinion_username,

```
....
57.                 HttpServletRequest request,
....
63.                 if(!captcha.validate(request, "opinionRecord_captcha",
model)){
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public boolean validate(HttpServletRequest request,String captcha_name,ModelMap model){

```
....
91.   public boolean validate(HttpServletRequest request,String
captcha_name,ModelMap model){
92.         String captcha = request.getParameter(captcha_name);
....
118.                    FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2712:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2712
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	57	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public void submit(String opinion_title,String opinion_username,

```
....
57.               HttpServletRequest request,
....
63.               if(!captcha.validate(request, "opinionRecord_captcha",
model)){
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public boolean validate(HttpServletRequest request,String captcha_name,ModelMap model){

```
....
91.   public boolean validate(HttpServletRequest request,String
captcha_name,ModelMap model){
92.         String captcha = request.getParameter(captcha_name);
....
118.                    FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2713:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2713
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	96	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String opinionRecord(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
96.   public String opinionRecord(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2714:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2714
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	96	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
96.   public String opinionRecord(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2715:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2715
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	96	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String opinionRecord(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
96.   public String opinionRecord(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2716:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2716
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String opinionRecord(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
96.   public String opinionRecord(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2717:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2717
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	96	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String opinionRecord(String id,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
96.   public String opinionRecord(String id,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2718:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2718
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	112	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
112.        public String list(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
114.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2719:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2719
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	112	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
112.        public String list(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
114.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2720:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2720
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	112	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
112.        public String list(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
114.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2721:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2721
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
112.        public String list(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
114.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2722:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2722
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	112	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
112.        public String list(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
114.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2723:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2723
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	177	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list_hdjl(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
177.        public String list_hdjl(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
179.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2724:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2724
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	177	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list_hdjl(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
177.        public String list_hdjl(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
179.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2725:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2725
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	177	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String list_hdjl(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
177.        public String list_hdjl(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
179.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2726:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2726
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	177	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String list_hdjl(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
177.        public String list_hdjl(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
179.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2727:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2727
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	177	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String list_hdjl(String title,Integer pageNo, HttpServletRequest request, ModelMap model) {

```
....
177.        public String list_hdjl(String title,Integer pageNo,
HttpServletRequest request, ModelMap model) {
....
179.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2728:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2728
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	190	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String openOpinion(String topicid, HttpServletRequest request, ModelMap model) {

```
....
190.        public String openOpinion(String topicid, HttpServletRequest
request, ModelMap model) {
....
193.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2729:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2729
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	190	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String openOpinion(String topicid, HttpServletRequest request, ModelMap model) {

```
....
190.        public String openOpinion(String topicid, HttpServletRequest
request, ModelMap model) {
....
193.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2730:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2730
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	190	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String openOpinion(String topicid, HttpServletRequest request, ModelMap model) {

```
....
190.        public String openOpinion(String topicid, HttpServletRequest
request, ModelMap model) {
....
193.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2731:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2731
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	190	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java
方法	public String openOpinion(String topicid, HttpServletRequest request, ModelMap model) {

```
....
190.        public String openOpinion(String topicid, HttpServletRequest
request, ModelMap model) {
....
193.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2732:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2732
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	190	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/OpinionRecordAct.java

方法 public String openOpinion(String topicid, HttpServletRequest request, ModelMap model) {

```
....
190.        public String openOpinion(String topicid, HttpServletRequest
request, ModelMap model) {
....
193.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2733:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2733
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	222	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdIndex(HttpServletRequest request,

```
....
222.        public String qzqdIndex( HttpServletRequest request,
....
225.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2734:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2734
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	222	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdIndex(HttpServletRequest request,

```
....
222.        public String qzqdIndex( HttpServletRequest request,
....
225.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2735:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2735
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	222	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java
方法	public String qzqdIndex(HttpServletRequest request,

```
....
222.        public String qzqdIndex( HttpServletRequest request,
....
225.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2736:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2736
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	222	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdIndex(HttpServletRequest request,

```
....
222.        public String qzqdIndex( HttpServletRequest request,
....
225.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2737:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2737
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	222	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdIndex(HttpServletRequest request,

```
....
222.        public String qzqdIndex( HttpServletRequest request,
....
225.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2738:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2738
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	25	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java

方法 public String index(HttpServletRequest request,

```
....
25.   public String index(HttpServletRequest request,
....
30.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2739:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2739
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	25	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java

方法 public String index(HttpServletRequest request,

```
....
25.   public String index(HttpServletRequest request,
....
30.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2740:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2740
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	25	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java
方法	public String index(HttpServletRequest request,

```
....
25.   public String index(HttpServletRequest request,
....
30.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2741:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2741
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	25	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java

方法 public String index(HttpServletRequest request,

```
....
25.   public String index(HttpServletRequest request,
....
30.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2742:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2742
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	25	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SearchAct.java

方法 public String index(HttpServletRequest request,

```
....
25.   public String index(HttpServletRequest request,
....
30.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2743:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2743
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	72	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toAdd(HttpServletRequest request,

```
....
72.   public String toAdd(HttpServletRequest request,
....
77.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2744:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2744
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	72	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toAdd(HttpServletRequest request,

```
....
72.   public String toAdd(HttpServletRequest request,
....
77.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2745:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2745
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	72	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java
方法	public String toAdd(HttpServletRequest request,

```
....
72.   public String toAdd(HttpServletRequest request,
....
77.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2746:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2746
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	72	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toAdd(HttpServletRequest request,

```
....
72.   public String toAdd(HttpServletRequest request,
....
77.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2747:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2747
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	72	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toAdd(HttpServletRequest request,

```
....
72.   public String toAdd(HttpServletRequest request,
....
77.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2748:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2748
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	99	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toEdit(String id,HttpServletRequest request,

```
....
99.   public String toEdit(String id,HttpServletRequest request,
....
109.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2749:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2749
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	99	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toEdit(String id,HttpServletRequest request,

```
....
99.   public String toEdit(String id,HttpServletRequest request,
....
109.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2750:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2750
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	99	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java
方法	public String toEdit(String id,HttpServletRequest request,

```
....
99.   public String toEdit(String id,HttpServletRequest request,
....
109.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2751:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2751
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	99	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toEdit(String id,HttpServletRequest request,

```
....
99.   public String toEdit(String id,HttpServletRequest request,
....
109.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2752:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2752
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	99	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String toEdit(String id,HttpServletRequest request,

```
....
99.   public String toEdit(String id,HttpServletRequest request,
....
109.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2753:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2753
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	31	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String index(HttpServletRequest request,

```
....
31.   public String index(HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2754:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2754
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	31	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String index(HttpServletRequest request,

```
....
31.   public String index(HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2755:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2755
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	31	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java
方法	public String index(HttpServletRequest request,

```
....
31.   public String index(HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2756:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2756
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	31	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String index(HttpServletRequest request,

```
....
31.   public String index(HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2757:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2757
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	31	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TagAct.java

方法 public String index(HttpServletRequest request,

```
....
31.   public String index(HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2758:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2758
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	31	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
31.   public String search(String linkname, HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2759:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2759
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	31	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
31.   public String search(String linkname, HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2760:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2760
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	31	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java
方法	public String search(String linkname, HttpServletRequest request,

```
....
31.   public String search(String linkname, HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2761:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2761
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	31	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
31.   public String search(String linkname, HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2762:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2762
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	31	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ToolAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
31.   public String search(String linkname, HttpServletRequest request,
....
34.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2763:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2763
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	42	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba(HttpServletRequest request,

```
....
42.   public String toTzspba( HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2764:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2764
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	42	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba(HttpServletRequest request,

```
....
42.   public String toTzspba( HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2765:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2765
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	42	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzspba(HttpServletRequest request,

```
....
42.   public String toTzspba( HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2766:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2766
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	42	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba(HttpServletRequest request,

```
....
42.   public String toTzspba( HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2767:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2767
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	42	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba(HttpServletRequest request,

```
....
42.   public String toTzspba( HttpServletRequest request,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2768:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2768
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	59	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba2(HttpServletRequest request,

```
....
59.   public String toTzspba2( HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2769:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2769
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba2(HttpServletRequest request,

```
....
59.   public String toTzspba2( HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2770:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2770
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzspba2(HttpServletRequest request,

```
....
59.   public String toTzspba2( HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2771:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2771
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba2(HttpServletRequest request,

```
....
59.   public String toTzspba2( HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2772:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2772
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba2(HttpServletRequest request,

```
....
59.   public String toTzspba2( HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2773:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2773
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	68	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba3(HttpServletRequest request,

```
....
68.   public String toTzspba3( HttpServletRequest request,
....
71.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2774:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2774
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	68	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba3(HttpServletRequest request,

```
....
68.   public String toTzspba3( HttpServletRequest request,
....
71.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2775:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2775
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	68	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzspba3(HttpServletRequest request,

```
....
68.   public String toTzspba3( HttpServletRequest request,
....
71.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2776:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2776
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	68	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba3(HttpServletRequest request,

```
....
68.   public String toTzspba3( HttpServletRequest request,
....
71.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2777:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2777
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	68	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba3(HttpServletRequest request,

```
....
68.   public String toTzspba3( HttpServletRequest request,
....
71.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2778:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2778
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	85	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp1(HttpServletRequest request,

```
....
85.   public String toTzsp1( HttpServletRequest request,
....
88.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2779:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2779
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	85	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp1(HttpServletRequest request,

```
....
85.   public String toTzsp1( HttpServletRequest request,
....
88.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2780:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2780
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	85	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzsp1(HttpServletRequest request,

```
....
85.   public String toTzsp1( HttpServletRequest request,
....
88.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2781:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2781
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	85	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp1(HttpServletRequest request,

```
....
85.   public String toTzsp1( HttpServletRequest request,
....
88.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2782:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2782
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	85	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp1(HttpServletRequest request,

```
....
85.   public String toTzsp1( HttpServletRequest request,
....
88.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2783:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2783
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	94	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp2(HttpServletRequest request,

```
....
94.   public String toTzsp2( HttpServletRequest request,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2784:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2784
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	94	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp2(HttpServletRequest request,

```
....
94.   public String toTzsp2( HttpServletRequest request,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2785:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2785
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	94	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzsp2(HttpServletRequest request,

```
....
94.   public String toTzsp2( HttpServletRequest request,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2786:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2786
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	94	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp2(HttpServletRequest request,

```
....
94.   public String toTzsp2( HttpServletRequest request,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2787:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2787
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	94	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp2(HttpServletRequest request,

```
....
94.   public String toTzsp2( HttpServletRequest request,
....
97.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2788:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2788
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	66	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdQZIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
66.   public String qzqdQZIndex(String[] types,String[] deptIds, Integer
pageNo,HttpServletRequest request,
....
69.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2789:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2789
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	66	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdQZIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
66.   public String qzqdQZIndex(String[] types,String[] deptIds, Integer
pageNo,HttpServletRequest request,
....
69.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2790:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2790
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	66	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdQZIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
66.   public String qzqdQZIndex(String[] types,String[] deptIds, Integer
pageNo,HttpServletRequest request,
....
69.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2791:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2791
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	66	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java
方法	public String qzqdQZIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
66.   public String qzqdQZIndex(String[] types,String[] deptIds, Integer
pageNo,HttpServletRequest request,
....
69.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2792:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2792
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	66	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdQZIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
66.   public String qzqdQZIndex(String[] types,String[] deptIds, Integer
pageNo,HttpServletRequest request,
....
69.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2793:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2793
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	103	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp3(HttpServletRequest request,

```
....
103.        public String toTzsp3( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2794:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2794
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp3(HttpServletRequest request,

```
....
103.        public String toTzsp3( HttpServletRequest request,
....
106.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2795:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2795
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp3(HttpServletRequest request,

```
....
103.        public String toTzsp3( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2796:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2796
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp3(HttpServletRequest request,

```
....
103.        public String toTzsp3( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2797:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2797
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp3(HttpServletRequest request,

```
....
103.        public String toTzsp3( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2798:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2798
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	107	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdBMIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
107.        public String qzqdBMIndex(String[] types,String[] deptIds,
Integer pageNo,HttpServletRequest request,
....
110.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2799:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2799
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	107	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdBMIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
107.        public String qzqdBMIndex(String[] types,String[] deptIds,
Integer pageNo,HttpServletRequest request,
....
110.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2800:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2800
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	107	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdBMIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
107.        public String qzqdBMIndex(String[] types,String[] deptIds,
Integer pageNo,HttpServletRequest request,
....
110.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2801:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2801
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	107	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java
方法	public String qzqdBMIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
107.        public String qzqdBMIndex(String[] types,String[] deptIds,
Integer pageNo,HttpServletRequest request,
....
110.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2802:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2802
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	107	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/QzqdAct.java

方法 public String qzqdBMIndex(String[] types,String[] deptIds, Integer pageNo,HttpServletRequest request,

```
....
107.        public String qzqdBMIndex(String[] types,String[] deptIds,
Integer pageNo,HttpServletRequest request,
....
110.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2803:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2803
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	63	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String list(Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
63.   public String list(     Integer pageNo,Integer pageSize,
HttpServletRequest request, ModelMap model) {
....
70.         String title = request.getParameter("title");
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2804:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2804
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	63	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String list(Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
63.   public String list(     Integer pageNo,Integer pageSize,
HttpServletRequest request, ModelMap model) {
....
70.         String title = request.getParameter("title");
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2805:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2805
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	63	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String list(Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
63.   public String list(     Integer pageNo,Integer pageSize,
HttpServletRequest request, ModelMap model) {
....
70.         String title = request.getParameter("title");
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2806:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2806
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	63	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java
方法	public String list(Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
63.   public String list(     Integer pageNo,Integer pageSize,
HttpServletRequest request, ModelMap model) {
....
70.         String title = request.getParameter("title");
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2807:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2807
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	63	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String list(Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
63.   public String list(     Integer pageNo,Integer pageSize,
HttpServletRequest request, ModelMap model) {
....
70.         String title = request.getParameter("title");
....
74.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2808:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2808
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	106	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
106.        public String result(Integer voteId, HttpServletRequest
request,
....
111.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2809:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2809
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	106	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
106.        public String result(Integer voteId, HttpServletRequest
request,
....
111.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2810:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2810
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	106	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
106.        public String result(Integer voteId, HttpServletRequest
request,
....
111.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2811:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2811
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java
方法	public String result(Integer voteId, HttpServletRequest request,

```
....
106.        public String result(Integer voteId, HttpServletRequest
request,
....
111.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2812:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2812
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	106	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
106.        public String result(Integer voteId, HttpServletRequest
request,
....
111.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2813:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2813
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	22	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java

方法 public String rss(HttpServletRequest request, HttpServletResponse response,

```
....
22.   public String rss(HttpServletRequest request, HttpServletResponse
response,
....
26.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2814:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2814
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	22	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java

方法 public String rss(HttpServletRequest request, HttpServletResponse response,

```
....
22.   public String rss(HttpServletRequest request, HttpServletResponse
response,
....
26.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2815:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2815
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	22	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java

方法 public String rss(HttpServletRequest request, HttpServletResponse response,

```
....
22.   public String rss(HttpServletRequest request, HttpServletResponse
response,
....
26.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2816:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2816
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	22	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java
方法	public String rss(HttpServletRequest request, HttpServletResponse response,

```
....
22.   public String rss(HttpServletRequest request, HttpServletResponse
response,
....
26.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2817:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2817
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	22	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RssAct.java

方法 public String rss(HttpServletRequest request, HttpServletResponse response,

```
....
22.   public String rss(HttpServletRequest request, HttpServletResponse
response,
....
26.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2818:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2818
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	58	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String List(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
58.   public String List( String queryTitle,Integer
pageNo,HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2819:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2819
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String List(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
58.   public String List( String queryTitle,Integer
pageNo,HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2820:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2820
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	58	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String List(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
58.   public String List( String queryTitle,Integer
pageNo,HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2821:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2821
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java
方法	public String List(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
58.   public String List( String queryTitle,Integer
pageNo,HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2822:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2822
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/SyncConfigAct.java

方法 public String List(String queryTitle,Integer pageNo,HttpServletRequest request,

```
....
58.   public String List( String queryTitle,Integer
pageNo,HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2823:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2823
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	46	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
46.   public String search(String linkname, HttpServletRequest request,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2824:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2824
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	46	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
46.   public String search(String linkname, HttpServletRequest request,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2825:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2825
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	46	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java
方法	public String search(String linkname, HttpServletRequest request,

```
....
46.   public String search(String linkname, HttpServletRequest request,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2826:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2826
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
46.   public String search(String linkname, HttpServletRequest request,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2827:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2827
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	46	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String search(String linkname, HttpServletRequest request,

```
....
46.   public String search(String linkname, HttpServletRequest request,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2828:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2828
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	110	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBJTJ(HttpServletRequest request,

```
....
110.        public String searchBJTJ(HttpServletRequest request,
....
113.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2829:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2829
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	110	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBJTJ(HttpServletRequest request,

```
....
110.        public String searchBJTJ(HttpServletRequest request,
....
113.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2830:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2830
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	110	272
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java
方法 public String searchBJTJ(HttpServletRequest request,

```
....
110.        public String searchBJTJ(HttpServletRequest request,
....
113.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2831:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2831
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	110	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBJTJ(HttpServletRequest request,

```
....
110.        public String searchBJTJ(HttpServletRequest request,
....
113.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2832:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2832
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	110	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchBJTJ(HttpServletRequest request,

```
....
110.        public String searchBJTJ(HttpServletRequest request,
....
113.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2833:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2833
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	119	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchMapLct(String linkname, HttpServletRequest request,

```
....
119.        public String searchMapLct(String linkname,
HttpServletRequest request,
....
122.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2834:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2834
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	119	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchMapLct(String linkname, HttpServletRequest request,

```
....
119.        public String searchMapLct(String linkname,
HttpServletRequest request,
....
122.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2835:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2835
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	119	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchMapLct(String linkname, HttpServletRequest request,

```
....
119.        public String searchMapLct(String linkname,
HttpServletRequest request,
....
122.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2836:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2836
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	119	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java
方法	public String searchMapLct(String linkname, HttpServletRequest request,

```
....
119.        public String searchMapLct(String linkname,
HttpServletRequest request,
....
122.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2837:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2837
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	119	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WebMapAct.java

方法 public String searchMapLct(String linkname, HttpServletRequest request,

```
....
119.        public String searchMapLct(String linkname,
HttpServletRequest request,
....
122.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2838:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2838
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	50	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba1(HttpServletRequest request,

```
....
50.   public String toTzspba1( HttpServletRequest request,
....
53.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2839:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2839
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	50	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba1(HttpServletRequest request,

```
....
50.   public String toTzspba1( HttpServletRequest request,
....
53.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2840:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2840
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	50	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzspba1(HttpServletRequest request,

```
....
50.   public String toTzspba1( HttpServletRequest request,
....
53.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2841:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2841
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	50	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba1(HttpServletRequest request,

```
....
50.   public String toTzspba1( HttpServletRequest request,
....
53.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2842:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2842
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	50	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzspba1(HttpServletRequest request,

```
....
50.   public String toTzspba1( HttpServletRequest request,
....
53.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2843:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2843
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	77	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp(HttpServletRequest request,

```
....
77.   public String toTzsp( HttpServletRequest request,
....
80.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2844:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2844
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	77	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp(HttpServletRequest request,

```
....
77.   public String toTzsp( HttpServletRequest request,
....
80.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2845:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2845
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	77	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java
方法	public String toTzsp(HttpServletRequest request,

```
....
77.   public String toTzsp( HttpServletRequest request,
....
80.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2846:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2846
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	77	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp(HttpServletRequest request,

```
....
77.   public String toTzsp( HttpServletRequest request,
....
80.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2847:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2847
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	77	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/TzspAct.java

方法 public String toTzsp(HttpServletRequest request,

```
....
77.   public String toTzsp( HttpServletRequest request,
....
80.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2848:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2848
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	132	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
132.        public String input(Integer voteId, HttpServletRequest
request,
....
139.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2849:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2849
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	132	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
132.        public String input(Integer voteId, HttpServletRequest
request,
....
139.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2850:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2850
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	132	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
132.        public String input(Integer voteId, HttpServletRequest
request,
....
139.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2851:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2851
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	132	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java
方法	public String input(Integer voteId, HttpServletRequest request,

```
....
132.        public String input(Integer voteId, HttpServletRequest
request,
....
139.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2852:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2852
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	132	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
132.        public String input(Integer voteId, HttpServletRequest
request,
....
139.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2853:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2853
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	161	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
161.                    HttpServletRequest request, HttpServletResponse
response,
....
196.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2854:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2854
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	161	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
161.                    HttpServletRequest request, HttpServletResponse
response,
....
196.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2855:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2855
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	161	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
161.                    HttpServletRequest request, HttpServletResponse
response,
....
196.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2856:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2856
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java
方法	public String submit(Integer voteId, Integer[] itemIds,

```
....
161.                    HttpServletRequest request, HttpServletResponse
response,
....
196.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2857:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2857
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/VoteAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
161.                    HttpServletRequest request, HttpServletResponse
response,
....
196.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2858:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2858
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	782	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matteredit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
782.        public String matteredit(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2859:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2859
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	782	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matteredit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
782.        public String matteredit(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2860:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2860
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	782	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matteredit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
782.        public String matteredit(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2861:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2861
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	782	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String matteredit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
782.        public String matteredit(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
785.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2862:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2862
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	782	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matteredit(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
782.        public String matteredit(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
785.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2863:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2863
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	984	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterdetail(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
984.        public String matterdetail(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
987.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2864:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2864
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	984	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterdetail(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
984.        public String matterdetail(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
987.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2865:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2865
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	984	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterdetail(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
984.        public String matterdetail(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
987.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2866:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2866
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	984	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String matterdetail(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
984.        public String matterdetail(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
987.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2867:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2867
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	984	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String matterdetail(String sxid, String bsnum, String redo, HttpServletRequest request,

```
....
984.        public String matterdetail(String sxid, String bsnum, String
redo, HttpServletRequest request,
....
987.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2868:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2868
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	58	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc1(HttpServletRequest request,

```
....
58.   public String toXnjc1( HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2869:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2869
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc1(HttpServletRequest request,

```
....
58.   public String toXnjc1( HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2870:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2870
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	58	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java
方法	public String toXnjc1(HttpServletRequest request,

```
....
58.   public String toXnjc1( HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2871:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2871
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc1(HttpServletRequest request,

```
....
58.   public String toXnjc1( HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2872:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2872
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	58	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc1(HttpServletRequest request,

```
....
58.   public String toXnjc1( HttpServletRequest request,
....
61.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2873:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2873
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	76	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc2(HttpServletRequest request,

```
....
76.   public String toXnjc2( HttpServletRequest request,
....
79.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2874:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2874
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc2(HttpServletRequest request,

```
....
76.   public String toXnjc2( HttpServletRequest request,
....
79.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2875:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2875
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	76	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java
方法	public String toXnjc2(HttpServletRequest request,

```
....
76.   public String toXnjc2( HttpServletRequest request,
....
79.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2876:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2876
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc2(HttpServletRequest request,

```
....
76.   public String toXnjc2( HttpServletRequest request,
....
79.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2877:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2877
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	76	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc2(HttpServletRequest request,

```
....
76.   public String toXnjc2( HttpServletRequest request,
....
79.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2878:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2878
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	91	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc3(HttpServletRequest request,

```
....
91.   public String toXnjc3( HttpServletRequest request,
....
94.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2879:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2879
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	91	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc3(HttpServletRequest request,

```
....
91.   public String toXnjc3( HttpServletRequest request,
....
94.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2880:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2880
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	91	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java
方法	public String toXnjc3(HttpServletRequest request,

```
....
91.   public String toXnjc3( HttpServletRequest request,
....
94.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2881:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2881
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	91	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc3(HttpServletRequest request,

```
....
91.   public String toXnjc3( HttpServletRequest request,
....
94.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2882:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2882
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	91	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc3(HttpServletRequest request,

```
....
91.   public String toXnjc3( HttpServletRequest request,
....
94.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2883:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2883
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	103	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
103.        public String zwgkIndex( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2884:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2884
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
103.        public String zwgkIndex( HttpServletRequest request,
....
106.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2885:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2885
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	103	272
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java
方法 public String zwgkIndex(HttpServletRequest request,

```
....
103.        public String zwgkIndex( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2886:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2886
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
103.        public String zwgkIndex( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2887:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2887
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	103	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String zwgkIndex(HttpServletRequest request,

```
....
103.        public String zwgkIndex( HttpServletRequest request,
....
106.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2888:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2888
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	153	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzgaItem(HttpServletRequest request,

```
....
153.        public String tzgaItem( HttpServletRequest request,
....
156.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2889:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2889
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	153	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzgaItem(HttpServletRequest request,

```
....
153.        public String tzgaItem( HttpServletRequest request,
....
156.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2890:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2890
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	153	272
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法 public String tzgaItem(HttpServletRequest request,

```
....
153.        public String tzgaItem( HttpServletRequest request,
....
156.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2891:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2891
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	153	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzgaItem(HttpServletRequest request,

```
....
153.        public String tzgaItem( HttpServletRequest request,
....
156.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2892:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2892
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	153	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzgaItem(HttpServletRequest request,

```
....
153.        public String tzgaItem( HttpServletRequest request,
....
156.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2893:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2893
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	161	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkItem(HttpServletRequest request,

```
....
161.        public String zwgkItem( HttpServletRequest request,
....
164.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2894:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2894
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	161	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkItem(HttpServletRequest request,

```
....
161.        public String zwgkItem( HttpServletRequest request,
....
164.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2895:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2895
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	161	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String zwgkItem(HttpServletRequest request,

```
....
161.        public String zwgkItem( HttpServletRequest request,
....
164.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2896:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2896
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkItem(HttpServletRequest request,

```
....
161.        public String zwgkItem( HttpServletRequest request,
....
164.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2897:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2897
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String zwgkItem(HttpServletRequest request,

```
....
161.        public String zwgkItem( HttpServletRequest request,
....
164.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2898:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2898
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	497	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
500.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2899:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2899
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	497	93
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
501.              String name = request.getParameter("selname");
502.              String deptid = request.getParameter("deptId");
....
540.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

SQL Injection\路径 2900:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2900
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	497	269
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
501.              String name = request.getParameter("selname");
....
506.                    name = name.replaceAll("《", "");
507.                    name = name.replaceAll("》", "");
508.                    name = name.trim();
....
536.              int
lawproduceCount=lawGuideMng.getLawproduceCount(com.jeecms.cms.CTools.get
StringAdd(name,"%"),deptid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.              if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                          sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public int getLawproduceCount(String name,String dept){

```
....
90.   public int getLawproduceCount(String name,String dept){
91.         return dao.getLawproduceCount(name,dept);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public int getLawproduceCount(String name,String dept) {

```
....
258.        public int getLawproduceCount(String name,String dept) {
....
261.              if(name != null && !name.equals("")){
262.                    sql += " and p.filename like '%"+name+"%' ";
....
266.              SQLQuery query=this.getSession().createSQLQuery(sql);
267.              query.setString(0, dept);
268.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
269.              List<Object> list=query.list();
```

SQL Injection\路径 2901:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2901
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	497	241
对象	request	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
500.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2902:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2902
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	497	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
500.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2903:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2903
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	497	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
500.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2904:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2904
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	497	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
497.        public String selawproduce(HttpServletRequest request,
....
500.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2905:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2905
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	145	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzga(HttpServletRequest request,

```
....
145.        public String tzga( HttpServletRequest request,
....
148.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2906:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2906
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	145	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzga(HttpServletRequest request,

```
....
145.        public String tzga( HttpServletRequest request,
....
148.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2907:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2907
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	145	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String tzga(HttpServletRequest request,

```
....
145.        public String tzga( HttpServletRequest request,
....
148.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2908:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2908
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzga(HttpServletRequest request,

```
....
145.        public String tzga( HttpServletRequest request,
....
148.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2909:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2909
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	145	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String tzga(HttpServletRequest request,

```
....
145.        public String tzga( HttpServletRequest request,
....
148.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2910:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2910
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	88	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String memberAuth(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
88.   public String memberAuth(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
92.         String username = request.getParameter("username") == null ?
"" : request.getParameter("username");
93.         String useruid = request.getParameter("useruid") == null ?
"" : request.getParameter("useruid");
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2911:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2911
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String memberAuth(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
88.   public String memberAuth(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
92.         String username = request.getParameter("username") == null ?
"" : request.getParameter("username");
93.         String useruid = request.getParameter("useruid") == null ?
"" : request.getParameter("useruid");
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2912:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2912
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	88	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String memberAuth(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
88.   public String memberAuth(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
92.         String username = request.getParameter("username") == null ?
"" : request.getParameter("username");
93.         String useruid = request.getParameter("useruid") == null ?
"" : request.getParameter("useruid");
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2913:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2913
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String memberAuth(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
88.   public String memberAuth(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
92.         String username = request.getParameter("username") == null ?
"" : request.getParameter("username");
93.         String useruid = request.getParameter("useruid") == null ?
"" : request.getParameter("useruid");
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2914:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2914
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	88	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String memberAuth(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws FileNotFoundException, IOException, SVSConnectException, ApplicationNotFoundException, InitException, ParameterOutRangeException, ParameterTooLongException {

```
....
88.   public String memberAuth(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws
FileNotFoundException, IOException, SVSConnectException,
ApplicationNotFoundException, InitException, ParameterOutRangeException,
ParameterTooLongException {
....
92.         String username = request.getParameter("username") == null ?
"" : request.getParameter("username");
93.         String useruid = request.getParameter("useruid") == null ?
"" : request.getParameter("useruid");
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2915:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2915
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	609	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String deny(HttpServletRequest request, ModelMap model) {

```
....
609.        public String deny(HttpServletRequest request, ModelMap
model) {
....
615.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2916:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2916
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	609	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String deny(HttpServletRequest request, ModelMap model) {

```
....
609.        public String deny(HttpServletRequest request, ModelMap
model) {
....
615.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2917:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2917
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	609	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String deny(HttpServletRequest request, ModelMap model) {

```
....
609.        public String deny(HttpServletRequest request, ModelMap
model) {
....
615.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2918:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2918
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	609	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java
方法	public String deny(HttpServletRequest request, ModelMap model) {

```
....
609.        public String deny(HttpServletRequest request, ModelMap
model) {
....
615.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2919:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2919
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	609	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CasLoginAct.java

方法 public String deny(HttpServletRequest request, ModelMap model) {

```
....
609.        public String deny(HttpServletRequest request, ModelMap
model) {
....
615.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2920:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2920
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	44	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc(HttpServletRequest request,

```
....
44.   public String toXnjc( HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2921:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2921
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc(HttpServletRequest request,

```
....
44.   public String toXnjc( HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2922:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2922
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	44	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java
方法	public String toXnjc(HttpServletRequest request,

```
....
44.   public String toXnjc( HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2923:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2923
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc(HttpServletRequest request,

```
....
44.   public String toXnjc( HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2924:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2924
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	44	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/XnjcAct.java

方法 public String toXnjc(HttpServletRequest request,

```
....
44.   public String toXnjc( HttpServletRequest request,
....
47.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2925:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2925
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	93	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public void collect_exist(Integer cId, HttpServletRequest request,

```
....
93.   public void collect_exist(Integer cId, HttpServletRequest request,
....
96.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2926:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2926
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	93	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public void collect_exist(Integer cId, HttpServletRequest request,

```
....
93.   public void collect_exist(Integer cId, HttpServletRequest request,
....
96.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2927:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2927
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	93	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public void collect_exist(Integer cId, HttpServletRequest request,

```
....
93.   public void collect_exist(Integer cId, HttpServletRequest request,
....
96.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2928:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2928
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	93	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java
方法	public void collect_exist(Integer cId, HttpServletRequest request,

```
....
93.   public void collect_exist(Integer cId, HttpServletRequest request,
....
96.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2929:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2929
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	93	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/CollectionMemberAct.java

方法 public void collect_exist(Integer cId, HttpServletRequest request,

```
....
93.   public void collect_exist(Integer cId, HttpServletRequest request,
....
96.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2930:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2930
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	547	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
551.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2931:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2931
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	547	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
551.                FrontUtils.frontData(request, model, site);
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2932:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2932
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	547	474
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
552.                String name  = request.getParameter("selname");
....
572.                Map<String, Object>
deptServerMap=lawGuideMng.getServiceRegisterByName(com.jeecms.cms.CTools
.getStringAdd(name,"%"),areaid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.                if (baseString != null &&
baseString.trim().length()>0) {
710.                        char[] chars = baseString.toCharArray();
....
713.                                sb.append(chars[i] + addString);
....
715.                        return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
124.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
125.                return dao.getServiceRegisterByName(sxzxname,areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
466.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
....
469.                                "from v_t_share_permissionitem bean
where  bean.areaid=? and bean.sxzxname like '%"+sxzxname+"%'";
....
468.              String sql="select count(1) serverCount,COUNT(CASE
WHEN bean.SFWSSB = 1 THEN 1  ELSE  NULL  END)  as wssbCount " +
....
471.              SQLQuery query=this.getSession().createSQLQuery(sql);
472.              query.setString(0, areaId);
473.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
474.              List<Object> list=query.list();
```

SQL Injection\路径 2933:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2933
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	547	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
551.              FrontUtils.frontData(request, model, site);
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2934:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2934

结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	547	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
551.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2935:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2935
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	547	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
547.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
551.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2936:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2936
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	903	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
903.        public String input(Integer voteId, HttpServletRequest
request,
....
908.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2937:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2937
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	903	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
903.        public String input(Integer voteId, HttpServletRequest
request,
....
908.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2938:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2938
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	903	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
903.        public String input(Integer voteId, HttpServletRequest
request,
....
908.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2939:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2939
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	903	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String input(Integer voteId, HttpServletRequest request,

```
....
903.        public String input(Integer voteId, HttpServletRequest
request,
....
908.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2940:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2940
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	903	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String input(Integer voteId, HttpServletRequest request,

```
....
903.        public String input(Integer voteId, HttpServletRequest
request,
....
908.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2941:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2941
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	930	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
930.                    HttpServletRequest request, HttpServletResponse
response,
....
965.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2942:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2942
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	930	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
930.                    HttpServletRequest request, HttpServletResponse
response,
....
965.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2943:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2943
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	930	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
930.                    HttpServletRequest request, HttpServletResponse
response,
....
965.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2944:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2944
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	930	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String submit(Integer voteId, Integer[] itemIds,

```
....
930.                    HttpServletRequest request, HttpServletResponse
response,
....
965.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2945:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2945
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	930	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String submit(Integer voteId, Integer[] itemIds,

```
....
930.                    HttpServletRequest request, HttpServletResponse
response,
....
965.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2946:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2946
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	979	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
979.        public String result(Integer voteId, HttpServletRequest
request,
....
984.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2947:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2947
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	979	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
979.        public String result(Integer voteId, HttpServletRequest
request,
....
984.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2948:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2948
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	979	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
979.        public String result(Integer voteId, HttpServletRequest
request,
....
984.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2949:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2949
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	979	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String result(Integer voteId, HttpServletRequest request,

```
....
979.        public String result(Integer voteId, HttpServletRequest
request,
....
984.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2950:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2950
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	979	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String result(Integer voteId, HttpServletRequest request,

```
....
979.        public String result(Integer voteId, HttpServletRequest
request,
....
984.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2951:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2951
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	585	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
589.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2952:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2952
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	585	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
589.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2953:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2953
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	585	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
589.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2954:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2954
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	585	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
589.                FrontUtils.frontData(request, model, site);
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2955:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2955
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	585	474
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
590.                String name  = request.getParameter("selname");
....
610.                Map<String, Object>
deptServerMap=lawGuideMng.getServiceRegisterByName(com.jeecms.cms.CTools
.getStringAdd(name,"%"),areaid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.                if (baseString != null &&
baseString.trim().length()>0) {
710.                        char[] chars = baseString.toCharArray();
....
713.                                sb.append(chars[i] + addString);
....
715.                        return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
124.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
125.                return dao.getServiceRegisterByName(sxzxname,areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
466.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
....
469.                                "from v_t_share_permissionitem bean
where  bean.areaid=? and bean.sxzxname like '%"+sxzxname+"%'";
....
468.                String sql="select count(1) serverCount,COUNT(CASE
WHEN bean.SFWSSB = 1 THEN 1  ELSE  NULL  END)  as wssbCount " +
....
471.                SQLQuery query=this.getSession().createSQLQuery(sql);
472.                query.setString(0, areaId);
473.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
474.                List<Object> list=query.list();
```

SQL Injection\路径 2956:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2956
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	585	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
585.        public String banshitingselpermissionitem(HttpServletRequest
request,
....
589.                FrontUtils.frontData(request, model, site);
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2957:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2957
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	136	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java
方法	public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
136.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
145.                String attachCode = request.getParameter("id");
....
149.                String clbh = request.getParameter("clbh");
....
174.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2958:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2958
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	136	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
136.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
145.              String attachCode = request.getParameter("id");
....
149.              String clbh = request.getParameter("clbh");
....
174.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 2959:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2959
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	136	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
136.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
145.                String attachCode = request.getParameter("id");
....
149.                String clbh = request.getParameter("clbh");
....
174.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2960:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2960
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	136	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
136.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
145.                String attachCode = request.getParameter("id");
....
149.                String clbh = request.getParameter("clbh");
....
174.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2961:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2961
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	136	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
136.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
145.                String attachCode = request.getParameter("id");
....
149.                String clbh = request.getParameter("clbh");
....
174.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2962:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2962
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	191	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
191.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
201.                String certCode = request.getParameter("id");
....
204.                String clbh = request.getParameter("clbh");
....
222.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2963:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2963
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	191	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
191.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
201.              String certCode = request.getParameter("id");
....
204.              String clbh = request.getParameter("clbh");
....
222.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2964:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2964
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	191	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
191.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
201.              String certCode = request.getParameter("id");
....
204.              String clbh = request.getParameter("clbh");
....
222.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2965:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2965
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	191	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java
方法	public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
191.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
201.                String certCode = request.getParameter("id");
....
204.                String clbh = request.getParameter("clbh");
....
222.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2966:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2966
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	191	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoAct.java
方法	public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
191.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
201.                String certCode = request.getParameter("id");
....
204.                String clbh = request.getParameter("clbh");
....
222.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2967:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2967
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	138	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String dataAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
138.        public String dataAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
147.                String attachCode = request.getParameter("id");
....
151.                String clbh = request.getParameter("clbh");
....
176.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2968:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2968
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	138	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String dataAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
138.        public String dataAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
147.              String attachCode = request.getParameter("id");
....
151.              String clbh = request.getParameter("clbh");
....
176.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2969:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2969
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	138	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String dataAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
138.        public String dataAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
147.              String attachCode = request.getParameter("id");
....
151.              String clbh = request.getParameter("clbh");
....
176.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2970:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2970
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String dataAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
138.        public String dataAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
147.                String attachCode = request.getParameter("id");
....
151.                String clbh = request.getParameter("clbh");
....
176.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2971:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2971
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	138	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String dataAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
138.        public String dataAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
147.              String attachCode = request.getParameter("id");
....
151.              String clbh = request.getParameter("clbh");
....
176.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2972:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2972
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	181	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
181.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
193.                String certCode = request.getParameter("id");
....
196.                String clbh = request.getParameter("clbh");
....
215.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2973:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2973
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	181	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
181.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
193.                String certCode = request.getParameter("id");
....
196.                String clbh = request.getParameter("clbh");
....
215.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2974:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2974
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	181	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
181.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
193.                String certCode = request.getParameter("id");
....
196.                String clbh = request.getParameter("clbh");
....
215.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2975:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2975
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	181	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
181.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
193.                String certCode = request.getParameter("id");
....
196.                String clbh = request.getParameter("clbh");
....
215.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2976:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2976
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	181	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseZiLiaoActgr.java
方法	public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
181.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
193.              String certCode = request.getParameter("id");
....
196.              String clbh = request.getParameter("clbh");
....
215.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2977:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2977
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	59	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordInput(HttpServletRequest request,

```
....
59.   public String forgotPasswordInput(HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2978:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2978
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	59	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordInput(HttpServletRequest request,

```
....
59.   public String forgotPasswordInput(HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2979:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2979
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	59	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordInput(HttpServletRequest request,

```
....
59.   public String forgotPasswordInput(HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2980:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2980
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java
方法	public String forgotPasswordInput(HttpServletRequest request,

```
....
59.   public String forgotPasswordInput(HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2981:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2981
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	59	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java

方法 public String forgotPasswordInput(HttpServletRequest request,

```
....
59.   public String forgotPasswordInput(HttpServletRequest request,
....
62.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2982:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2982
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	28	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java

方法 public String csi(HttpServletRequest request, ModelMap model) {

```
....
28.   public String csi(HttpServletRequest request, ModelMap model) {
....
32.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2983:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2983
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	28	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java

方法 public String csi(HttpServletRequest request, ModelMap model) {

```
....
28.   public String csi(HttpServletRequest request, ModelMap model) {
....
32.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java
方法	public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2984:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2984
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	28	272
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java
方法	public String csi(HttpServletRequest request, ModelMap model) {

```
....
28.   public String csi(HttpServletRequest request, ModelMap model) {
....
32.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2985:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2985
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	28	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java

方法 public String csi(HttpServletRequest request, ModelMap model) {

```
....
28.   public String csi(HttpServletRequest request, ModelMap model) {
....
32.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 2986:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2986
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	28	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/LoginAct.java

方法 public String csi(HttpServletRequest request, ModelMap model) {

```
....
28.   public String csi(HttpServletRequest request, ModelMap model) {
....
32.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2987:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2987
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	695	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String shiyongbangzhu(Integer id, HttpServletRequest request,

```
....
695.        public String shiyongbangzhu(Integer id, HttpServletRequest
request,
....
698.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2988:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2988
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	695	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String shiyongbangzhu(Integer id, HttpServletRequest request,

```
....
695.        public String shiyongbangzhu(Integer id, HttpServletRequest
request,
....
698.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2989:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2989
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	695	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String shiyongbangzhu(Integer id, HttpServletRequest request,

```
....
695.        public String shiyongbangzhu(Integer id, HttpServletRequest
request,
....
698.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2990:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2990
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	695	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java
方法	public String shiyongbangzhu(Integer id, HttpServletRequest request,

```
....
695.        public String shiyongbangzhu(Integer id, HttpServletRequest
request,
....
698.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2991:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2991
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	695	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String shiyongbangzhu(Integer id, HttpServletRequest request,

```
....
695.        public String shiyongbangzhu(Integer id, HttpServletRequest
request,
....
698.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2992:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2992
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	704	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String wangzhanditu(Integer id, HttpServletRequest request,

```
....
704.        public String wangzhanditu(Integer id, HttpServletRequest
request,
....
707.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2993:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2993
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	704	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String wangzhanditu(Integer id, HttpServletRequest request,

```
....
704.        public String wangzhanditu(Integer id, HttpServletRequest
request,
....
707.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2994:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2994
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	704	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String wangzhanditu(Integer id, HttpServletRequest request,

```
....
704.        public String wangzhanditu(Integer id, HttpServletRequest
request,
....
707.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2995:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2995
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	704	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java
方法	public String wangzhanditu(Integer id, HttpServletRequest request,

```
....
704.        public String wangzhanditu(Integer id, HttpServletRequest
request,
....
707.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 2996:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2996
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	704	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String wangzhanditu(Integer id, HttpServletRequest request,

```
....
704.        public String wangzhanditu(Integer id, HttpServletRequest
request,
....
707.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 2997:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2997
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	713	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String lianxiwomen(Integer id, HttpServletRequest request,

```
....
713.        public String lianxiwomen(Integer id, HttpServletRequest
request,
....
716.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 2998:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2998
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	713	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String lianxiwomen(Integer id, HttpServletRequest request,

```
....
713.        public String lianxiwomen(Integer id, HttpServletRequest
request,
....
716.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 2999:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=2999
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	713	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String lianxiwomen(Integer id, HttpServletRequest request,

```
....
713.        public String lianxiwomen(Integer id, HttpServletRequest
request,
....
716.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3000:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3000
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	713	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java
方法	public String lianxiwomen(Integer id, HttpServletRequest request,

```
....
713.        public String lianxiwomen(Integer id, HttpServletRequest
request,
....
716.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3001:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3001
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	713	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MessageAct.java

方法 public String lianxiwomen(Integer id, HttpServletRequest request,

```
....
713.        public String lianxiwomen(Integer id, HttpServletRequest
request,
....
716.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3002:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3002
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	48	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
66.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3003:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3003
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	48	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
66.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3004:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3004
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	48	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
66.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3005:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3005
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java
方法	public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
66.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3006:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3006
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	48	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java
方法	public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
66.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3007:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3007
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	48	261
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.                 String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.               return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
260.              String sxNameSql = "select t.sxname from
t_share_permissionitem t where t.id='"+sxid+ "'";
261.              List
list=sessionFactory.openSession().createSQLQuery(sxNameSql).list();
```

SQL Injection\路径 3008:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3008
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	48	271
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
48.   public String getclInfo(HttpServletRequest request, ModelMap
model) {
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.               String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java
方法	public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.               return request.getParameter(name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
269.                           + sxid + "'";
....
268.              String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver,c.patterninstid
fid,c.orinum,c.copynum,c.clbh,t.sfby,c.bz,t.ordernum from t_share_sxclgl
t,t_share_clxx c where c.id = t.clid and c.dzhyq<>'1' and (t.changetype
is null or t.changetype = 'C' or t.changetype = 'U') and t.sxid='"
....
271.              for (Object o
:sessionFactory.openSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3009:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3009
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	129	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java
方法	public String toSuccess(HttpServletRequest request, ModelMap model) {

```
....
129.        public String toSuccess(HttpServletRequest request, ModelMap
model) {
....
131.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3010:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3010
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String toSuccess(HttpServletRequest request, ModelMap model) {

```
....
129.        public String toSuccess(HttpServletRequest request, ModelMap
model) {
....
131.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 3011:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3011
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	129	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String toSuccess(HttpServletRequest request, ModelMap model) {

```
....
129.        public String toSuccess(HttpServletRequest request, ModelMap
model) {
....
131.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3012:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3012
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	218
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String toSuccess(HttpServletRequest request, ModelMap model) {

```
....
129.        public String toSuccess(HttpServletRequest request, ModelMap
model) {
....
131.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3013:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3013
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	129	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String toSuccess(HttpServletRequest request, ModelMap model) {

```
....
129.        public String toSuccess(HttpServletRequest request, ModelMap
model) {
....
131.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3014:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3014
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	109	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
109.        public String selpermissionitem(HttpServletRequest request,
....
112.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3015:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3015
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	109	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
109.        public String selpermissionitem(HttpServletRequest request,
....
112.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3016:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3016
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	109	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
109.        public String selpermissionitem(HttpServletRequest request,
....
112.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3017:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3017
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	109	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java
方法	public String selpermissionitem(HttpServletRequest request,

```
....
109.        public String selpermissionitem(HttpServletRequest request,
....
112.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3018:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3018
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	109	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String selpermissionitem(HttpServletRequest request,

```
....
109.        public String selpermissionitem(HttpServletRequest request,
....
112.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3019:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3019
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	290	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
290.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
294.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3020:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3020
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	290	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
290.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
294.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3021:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3021
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	290	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java

方法 public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
290.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
294.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3022:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3022
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	290	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java
方法	public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
290.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
294.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3023:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3023
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	290	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/PermissionAct.java
方法	public String permsort_00(String parentid,HttpServletRequest request, HttpServletResponse response,

```
....
290.        public String permsort_00(String parentid,HttpServletRequest
request, HttpServletResponse response,
....
294.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3024:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3024
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	614	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String downloadFile(HttpServletRequest request,

```
....
614.        public String downloadFile(HttpServletRequest request,
....
617.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3025:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3025
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	614	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String downloadFile(HttpServletRequest request,

```
....
614.        public String downloadFile(HttpServletRequest request,
....
617.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3026:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3026
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	614	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String downloadFile(HttpServletRequest request,

```
....
614.        public String downloadFile(HttpServletRequest request,
....
617.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3027:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3027
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	614	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java
方法	public String downloadFile(HttpServletRequest request,

```
....
614.        public String downloadFile(HttpServletRequest request,
....
617.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3028:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3028
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	614	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegisterAct.java

方法 public String downloadFile(HttpServletRequest request,

```
....
614.        public String downloadFile(HttpServletRequest request,
....
617.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3029:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3029
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	97	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3030:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3030
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	97	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3031:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3031
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	97	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3032:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3032
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	97	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java
方法	public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3033:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3033
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	97	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java
方法	public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
99.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3034:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3034
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	134	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String jdchaxun(Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model){

```
....
134.        public String jdchaxun(Integer pageNo,HttpServletRequest
request, HttpServletResponse response,ModelMap model){
....
136.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3035:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3035
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	134	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String jdchaxun(Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model){

```
....
134.        public String jdchaxun(Integer pageNo,HttpServletRequest
request, HttpServletResponse response,ModelMap model){
....
136.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3036:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3036
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	134	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String jdchaxun(Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model){

```
....
134.        public String jdchaxun(Integer pageNo,HttpServletRequest
request, HttpServletResponse response,ModelMap model){
....
136.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3037:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3037
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	134	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java
方法	public String jdchaxun(Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model){

```
....
134.        public String jdchaxun(Integer pageNo,HttpServletRequest
request, HttpServletResponse response,ModelMap model){
....
136.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3038:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3038
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	134	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java
方法	public String jdchaxun(Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model){

```
....
134.        public String jdchaxun(Integer pageNo,HttpServletRequest
request, HttpServletResponse response,ModelMap model){
....
136.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3039:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3039
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	155	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyezhuce(HttpServletRequest request, ModelMap model) {

```
....
155.        public String qiyezhuce(HttpServletRequest request, ModelMap
model) {
....
157.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3040:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3040
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	155	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyezhuce(HttpServletRequest request, ModelMap model) {

```
....
155.        public String qiyezhuce(HttpServletRequest request, ModelMap
model) {
....
157.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                        if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3041:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3041
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	155	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyezhuce(HttpServletRequest request, ModelMap model) {

```
....
155.        public String qiyezhuce(HttpServletRequest request, ModelMap
model) {
....
157.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3042:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3042
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	155	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java
方法	public String qiyezhuce(HttpServletRequest request, ModelMap model) {

```
....
155.        public String qiyezhuce(HttpServletRequest request, ModelMap
model) {
....
157.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3043:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3043
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	155	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyezhuce(HttpServletRequest request, ModelMap model) {

```
....
155.        public String qiyezhuce(HttpServletRequest request, ModelMap
model) {
....
157.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3044:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3044
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	108	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
108.      public String input(HttpServletRequest request, ModelMap
model) {
....
111.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3045:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3045
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	108	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
108.      public String input(HttpServletRequest request, ModelMap
model) {
....
111.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3046:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3046
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	108	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
108.      public String input(HttpServletRequest request, ModelMap
model) {
....
111.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3047:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3047
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	108	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String input(HttpServletRequest request, ModelMap model) {

```
....
108.      public String input(HttpServletRequest request, ModelMap
model) {
....
111.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3048:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3048
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	108	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String input(HttpServletRequest request, ModelMap model) {

```
....
108.      public String input(HttpServletRequest request, ModelMap
model) {
....
111.          FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3049:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3049
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	161	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
161.        public String
companyApplicationFormDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
164.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3050:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3050
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	161	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
161.        public String
companyApplicationFormDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
164.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3051:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3051
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	161	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
161.        public String
companyApplicationFormDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
164.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3052:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3052
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
161.        public String
companyApplicationFormDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
164.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3053:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3053
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	161	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
161.        public String
companyApplicationFormDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
164.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3054:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3054
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	179	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
179.        public String
companyApplicationFormDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
182.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3055:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3055
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	179	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
179.        public String
companyApplicationFormDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
182.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3056:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3056
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	179	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
179.        public String
companyApplicationFormDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
182.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3057:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3057
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	179	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
179.        public String
companyApplicationFormDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
182.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3058:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3058
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	179	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
179.        public String
companyApplicationFormDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
182.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3059:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3059
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	197	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
197.        public String companyApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3060:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3060
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	197	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
197.        public String companyApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3061:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3061
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	197	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
197.        public String companyApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3062:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3062
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	197	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
197.        public String companyApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3063:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3063
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	197	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
197.        public String companyApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3064:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3064
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	215	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
215.        public String companyAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
218.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3065:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3065
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	215	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
215.        public String companyAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
218.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3066:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3066
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	215	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
215.        public String companyAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
218.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3067:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3067
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	215	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
215.        public String companyAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
218.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3068:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3068
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	215	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
215.        public String companyAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
218.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3069:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3069
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	235	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
235.        public String companyAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
238.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3070:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3070
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	235	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
235.        public String companyAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
238.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3071:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3071
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	235	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
235.        public String companyAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
238.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3072:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3072
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	235	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
235.        public String companyAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
238.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3073:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3073
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	235	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
235.        public String companyAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
238.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3074:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3074
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	253	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
253.        public String companyAttachmentList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
256.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3075:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3075
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	253	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
253.        public String companyAttachmentList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
256.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3076:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3076
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	253	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
253.        public String companyAttachmentList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
256.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3077:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3077
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	253	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
253.        public String companyAttachmentList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
256.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3078:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3078
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	253	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
253.        public String companyAttachmentList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
256.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3079:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3079
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	271	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
271.        public String companyBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
274.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3080:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3080
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	271	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
271.        public String companyBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
274.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3081:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3081
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	271	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
271.        public String companyBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
274.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3082:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3082
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	271	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
271.        public String companyBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
274.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3083:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3083
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	271	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
271.        public String companyBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
274.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3084:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3084
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	289	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
289.        public String companyCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
292.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3085:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3085
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	289	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
289.        public String companyCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
292.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3086:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3086
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	289	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
289.        public String companyCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
292.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3087:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3087
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	289	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
289.        public String companyCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
292.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3088:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3088
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	289	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
289.        public String companyCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
292.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3089:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3089
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	307	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
307.        public String companyCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
310.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3090:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3090
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	307	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
307.        public String companyCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
310.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3091:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3091
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	307	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
307.        public String companyCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
310.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3092:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3092
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	307	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
307.        public String companyCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
310.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3093:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3093
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	307	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
307.        public String companyCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
310.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3094:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3094
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	325	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
325.        public String companyCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
328.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3095:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3095
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	325	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
325.        public String companyCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
328.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3096:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3096
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	325	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
325.        public String companyCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
328.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3097:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3097
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	325	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
325.        public String companyCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
328.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3098:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3098
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	325	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
325.        public String companyCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
328.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3099:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3099
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	343	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
343.        public String companyRecordDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
346.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3100:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3100
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	343	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
343.        public String companyRecordDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
346.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3101:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3101
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	343	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
343.        public String companyRecordDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
346.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3102:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3102
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	343	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
343.        public String companyRecordDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
346.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3103:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3103
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	343	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
343.        public String companyRecordDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
346.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3104:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3104
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	361	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
361.        public String companyRecordDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
364.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3105:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3105
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	361	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
361.        public String companyRecordDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
364.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3106:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3106
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	361	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
361.        public String companyRecordDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
364.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3107:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3107
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	361	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
361.        public String companyRecordDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
364.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3108:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3108
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	361	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
361.        public String companyRecordDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
364.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3109:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3109
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	379	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
379.        public String companyRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
382.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3110:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3110
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	379	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
379.        public String companyRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
382.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3111:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3111
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	379	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
379.        public String companyRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
382.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3112:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3112
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	379	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java
方法	public String companyRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
379.        public String companyRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
382.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3113:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3113
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	379	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceCompanyAct.java

方法 public String companyRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
379.        public String companyRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
382.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3114:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3114
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	196	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
196.        public String userApplicationFormDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3115:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3115
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	196	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
196.        public String userApplicationFormDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3116:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3116
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	196	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
196.        public String userApplicationFormDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3117:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3117
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	196	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
196.        public String userApplicationFormDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3118:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3118
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	196	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userApplicationFormDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
196.        public String userApplicationFormDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
200.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3119:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3119
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	214	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
214.        public String userApplicationFormDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
221.                String attachCode = request.getParameter("id");
....
225.                String clbh = request.getParameter("clbh");
....
247.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3120:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3120
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	214	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
214.        public String userApplicationFormDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
221.              String attachCode = request.getParameter("id");
....
225.              String clbh = request.getParameter("clbh");
....
247.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3121:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3121
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	214	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
214.        public String userApplicationFormDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
221.              String attachCode = request.getParameter("id");
....
225.              String clbh = request.getParameter("clbh");
....
247.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3122:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3122
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	214	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
214.        public String userApplicationFormDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
221.                String attachCode = request.getParameter("id");
....
225.                String clbh = request.getParameter("clbh");
....
247.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3123:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3123
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	214	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userApplicationFormDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
214.        public String userApplicationFormDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
221.              String attachCode = request.getParameter("id");
....
225.              String clbh = request.getParameter("clbh");
....
247.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3124:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3124
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	261	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
261.        public String userApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
284.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3125:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3125
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	261	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
261.        public String userApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
284.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3126:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3126
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	261	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
261.        public String userApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
284.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3127:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3127
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	261	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
261.        public String userApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
284.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3128:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3128
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	261	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userApplicationFormList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
261.        public String userApplicationFormList(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
284.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3129:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3129
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	298	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAllDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
298.        public String userAllDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
424.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3130:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3130
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	298	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAllDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
298.        public String userAllDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
424.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3131:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3131
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	298	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAllDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
298.        public String userAllDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
424.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3132:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3132
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	298	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAllDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
298.        public String userAllDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
424.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3133:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3133
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	298	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAllDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
298.        public String userAllDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
424.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3134:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3134
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	458	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
458.        public String userAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3135:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3135
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	458	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
458.        public String userAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
462.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3136:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3136
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	458	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
458.        public String userAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
462.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3137:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3137
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	458	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
458.        public String userAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
462.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3138:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3138
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	458	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
458.        public String userAttachmentDelete(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
462.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3139:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3139
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	476	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
476.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
486.                String attachCode = request.getParameter("id");
....
490.                String clbh = request.getParameter("clbh");
....
515.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3140:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3140
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	476	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
476.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
486.              String attachCode = request.getParameter("id");
....
490.              String clbh = request.getParameter("clbh");
....
515.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3141:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3141
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	476	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
476.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
486.              String attachCode = request.getParameter("id");
....
490.              String clbh = request.getParameter("clbh");
....
515.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3142:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3142
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	476	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
476.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
486.                String attachCode = request.getParameter("id");
....
490.                String clbh = request.getParameter("clbh");
....
515.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3143:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3143
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	476	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
476.        public String userAttachmentDetail(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
486.                String attachCode = request.getParameter("id");
....
490.                String clbh = request.getParameter("clbh");
....
515.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3144:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3144
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	520	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
520.        public String userAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
530.                String attachCode = request.getParameter("id");
....
534.                String clbh = request.getParameter("clbh");
....
559.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3145:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3145
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	520	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
520.        public String userAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
530.                String attachCode = request.getParameter("id");
....
534.                String clbh = request.getParameter("clbh");
....
559.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3146:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3146
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	520	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
520.        public String userAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
530.              String attachCode = request.getParameter("id");
....
534.              String clbh = request.getParameter("clbh");
....
559.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3147:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3147
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	520	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
520.        public String userAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
530.                String attachCode = request.getParameter("id");
....
534.                String clbh = request.getParameter("clbh");
....
559.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3148:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3148
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	520	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
520.        public String userAttachmentDetailgr(HttpServletRequest
request, HttpServletResponse response, ModelMap model) {
....
530.                String attachCode = request.getParameter("id");
....
534.                String clbh = request.getParameter("clbh");
....
559.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3149:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3149
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	572	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
572.        public String userAttachmentList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
585.                String attachCode = request.getParameter("id");
586.                String clbh = request.getParameter("clbh");
....
603.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3150:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3150
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	572	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
572.        public String userAttachmentList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
585.                String attachCode = request.getParameter("id");
586.                String clbh = request.getParameter("clbh");
....
603.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3151:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3151
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	572	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
572.        public String userAttachmentList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
585.              String attachCode = request.getParameter("id");
586.              String clbh = request.getParameter("clbh");
....
603.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3152:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3152
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	572	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
572.        public String userAttachmentList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
585.                String attachCode = request.getParameter("id");
586.                String clbh = request.getParameter("clbh");
....
603.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3153:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3153
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	572	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAttachmentList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
572.        public String userAttachmentList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
585.              String attachCode = request.getParameter("id");
586.              String clbh = request.getParameter("clbh");
....
603.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3154:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3154
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	617	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
617.        public String userBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
629.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3155:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3155
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	617	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
617.        public String userBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
629.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3156:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3156
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	617	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
617.        public String userBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
629.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3157:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3157
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	617	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
617.        public String userBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
629.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3158:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3158
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	617	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userBaseDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
617.        public String userBaseDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
629.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3159:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3159
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	643	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
643.        public String userCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
647.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3160:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3160
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	643	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
643.        public String userCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
647.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3161:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3161
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	643	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
643.        public String userCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
647.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3162:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3162
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	643	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
643.        public String userCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
647.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3163:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3163
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	643	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
643.        public String userCertDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
647.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3164:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3164
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	661	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
661.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
674.                String certCode = request.getParameter("id");
....
677.                String clbh = request.getParameter("clbh");
....
696.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3165:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3165
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	661	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
661.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
674.                String certCode = request.getParameter("id");
....
677.                String clbh = request.getParameter("clbh");
....
696.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3166:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3166
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	661	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
661.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
674.                String certCode = request.getParameter("id");
....
677.                String clbh = request.getParameter("clbh");
....
696.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3167:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3167
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	661	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
661.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
674.                String certCode = request.getParameter("id");
....
677.                String clbh = request.getParameter("clbh");
....
696.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3168:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3168
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	661	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
661.        public String userCertDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
674.              String certCode = request.getParameter("id");
....
677.              String clbh = request.getParameter("clbh");
....
696.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3169:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3169
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	701	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
701.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
714.                String certCode = request.getParameter("id");
....
717.                String clbh = request.getParameter("clbh");
....
736.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3170:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3170
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	701	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
701.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
714.                String certCode = request.getParameter("id");
....
717.                String clbh = request.getParameter("clbh");
....
736.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3171:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3171
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	701	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
701.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
714.                String certCode = request.getParameter("id");
....
717.                String clbh = request.getParameter("clbh");
....
736.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3172:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3172
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	701	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
701.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
714.                String certCode = request.getParameter("id");
....
717.                String clbh = request.getParameter("clbh");
....
736.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3173:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3173
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	701	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertDetailgr(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
701.        public String userCertDetailgr(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
714.              String certCode = request.getParameter("id");
....
717.              String clbh = request.getParameter("clbh");
....
736.              FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3174:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3174
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	797	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
797.        public String userCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
823.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3175:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3175
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	797	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
797.        public String userCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3176:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3176
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	797	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
797.        public String userCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3177:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3177
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	797	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
797.        public String userCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
823.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3178:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3178
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	797	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
797.        public String userCertList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
823.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3179:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3179
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	844	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList2(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
844.        public String userCertList2(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
868.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3180:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3180
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	844	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList2(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
844.        public String userCertList2(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
868.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3181:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3181
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	844	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userCertList2(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
844.        public String userCertList2(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
868.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3182:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3182
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	844	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertList2(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
844.        public String userCertList2(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
868.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3183:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3183
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	844	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userCertList2(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
844.        public String userCertList2(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
868.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3184:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3184
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	882	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
882.        public String userRecordDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
886.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3185:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3185
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	882	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
882.        public String userRecordDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
886.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3186:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3186
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	882	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
882.        public String userRecordDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
886.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3187:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3187
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	882	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
882.        public String userRecordDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
886.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3188:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3188
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	882	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userRecordDelete(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
882.        public String userRecordDelete(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
886.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3189:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3189
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	900	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
900.        public String userRecordDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
907.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3190:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3190
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	900	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
900.        public String userRecordDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
907.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3191:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3191
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	900	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
900.        public String userRecordDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
907.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3192:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3192
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	900	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
900.        public String userRecordDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
907.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3193:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3193
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	900	247
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordDetail(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
900.        public String userRecordDetail(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
907.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3194:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3194
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	934	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
934.        public String userRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
946.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3195:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3195
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	934	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
934.        public String userRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
946.            FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.            Long startTime = (Long)
request.getAttribute(START_TIME);
325.            String areaId = request.getParameter("areaId");
....
327.            if(areaId != null && !areaId.equals("")){
....
329.                if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3196:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3196
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	934	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
934.        public String userRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
946.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3197:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3197
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	934	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
934.        public String userRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
946.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3198:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3198
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	934	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userRecordList(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
934.        public String userRecordList(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
946.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3199:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3199
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	1155	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAffairsCount(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
1155.       public String userAffairsCount(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
1159.               FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3200:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3200
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	1155	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAffairsCount(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
1155.       public String userAffairsCount(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
1159.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3201:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3201
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	1155	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java

方法 public String userAffairsCount(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
1155.       public String userAffairsCount(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
1159.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3202:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3202
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1155	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAffairsCount(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
1155.       public String userAffairsCount(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
1159.             FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3203:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3203
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	1155	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceUserAct.java
方法	public String userAffairsCount(HttpServletRequest request, HttpServletResponse response, ModelMap model) {

```
....
1155.       public String userAffairsCount(HttpServletRequest request,
HttpServletResponse response, ModelMap model) {
....
1159.             FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3204:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3204
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	36	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
40.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3205:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3205
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	36	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
40.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3206:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3206
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	36	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
40.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3207:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3207
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
40.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3208:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3208
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	36	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
36.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
40.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3209:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3209
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3210:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3210
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3211:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3211
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3212:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3212
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3213:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3213
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3214:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3214
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	272	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
275.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3215:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3215
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	272	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
275.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3216:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3216
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	272	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
275.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3217:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3217
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	272	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
275.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3218:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3218
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	272	247
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java
方法	public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
275.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3219:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3219
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	45	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3220:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3220
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	45	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3221:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3221
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	45	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3222:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3222
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	45	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3223:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3223
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	45	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
45.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
49.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3224:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3224
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	318	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
322.                FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3225:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3225
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	318	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
322.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3226:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3226
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	318	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
322.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3227:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3227
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	318	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
322.              FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3228:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3228
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	318	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String enterprisegrStorePermBySxid(String sxid,String sxzxname,String sortcode,String areaId,HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
318.        public String enterprisegrStorePermBySxid(String sxid,String
sxzxname,String sortcode,String areaId,HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
322.                FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3229:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3229
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	41	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3230:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3230
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	41	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3231:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3231
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	41	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.                Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3232:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3232
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3233:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3233
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	41	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
41.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
45.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3234:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3234
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3235:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3235
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3236:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3236
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3237:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3237
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

SQL Injection\路径 3238:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3238
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3239:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3239
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	35	37
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                      Object areaId =
request.getSession().getAttribute("areaId");
....
113.                      List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3240:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3240
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	35	241
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

SQL Injection\路径 3241:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3241
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

行	35	272
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3242:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3242
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	218
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.                Long startTime = (Long)
request.getAttribute(START_TIME);
325.                String areaId = request.getParameter("areaId");
....
327.                if(areaId != null && !areaId.equals("")){
....
329.                      if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.                String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.                Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3243:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3243
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	35	247
对象	request	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java
方法	public String tableList(String areaId,HttpServletRequest request, HttpServletResponse response,

```
....
35.   public String tableList(String areaId,HttpServletRequest request,
HttpServletResponse response,
....
39.         FrontUtils.frontData(request, model, site);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static void frontData(HttpServletRequest request,

```
....
320.        public static void frontData(HttpServletRequest request,
....
324.              Long startTime = (Long)
request.getAttribute(START_TIME);
325.              String areaId = request.getParameter("areaId");
....
327.              if(areaId != null && !areaId.equals("")){
....
329.                    if(areaId.matches("[0-9]+")){
330.
      request.getSession().setAttribute("areaId", areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3244:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3244
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	309	37
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZxTwo(String sxid,HttpServletRequest request,

```
....
309.                    String areaId = request.getParameter("areaId");
....
311.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3245:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3245
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	330	37
对象	""areaId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddTsTwo(String deptid,HttpServletRequest request,

```
....
330.                   String areaId = request.getParameter("areaId");
....
332.                   List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java
方法	public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
方法	public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

SQL Injection\路径 3246:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3246
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	246	93
对象	deptid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String list(String deptid, String permtype,

```
....
246.        public String list(String deptid, String permtype,
....
275.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

SQL Injection\路径 3247:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3247
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	391	93
对象	deptid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
391.        public String lawproduceList(String deptid, String permtype,
....
489.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java
方法	public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
方法	public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

SQL Injection\路径 3248:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3248
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	391	36
对象	deptid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String lawproduceList(String deptid, String permtype,

```
....
391.        public String lawproduceList(String deptid, String permtype,
....
411.              List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptid,name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
方法	public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 3249:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3249
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	502	93
对象	""deptId""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String selawproduce(HttpServletRequest request,

```
....
502.              String deptid = request.getParameter("deptId");
....
540.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java
方法	public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
方法	public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

SQL Injection\路径 3250:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3250
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	663	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
663.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
681.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.                sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.                Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.                querycount.setCacheable(false);
133.                List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java
方法	public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3251:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3251
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	663	165
对象	""bsnum""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java
方法	public String done(HttpServletRequest request,

```
....
663.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
681.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3252:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3252
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	698	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
698.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
716.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3253:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3253
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	698	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
698.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
716.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3254:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3254
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	625	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
625.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
645.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3255:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3255
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	625	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
625.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
645.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3256:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3256
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	673	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
673.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
679.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3257:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3257
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	673	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
673.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
679.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3258:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3258
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	705	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
705.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
709.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3259:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3259
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	705	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
705.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
709.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3260:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3260
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	735	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
735.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
739.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3261:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3261
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	735	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
735.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
739.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3262:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3262
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	766	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
766.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
770.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3263:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3263
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	766	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
766.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
770.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3264:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3264
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	734	133
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
734.                String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
753.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
123.                    sbcount.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3265:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3265
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	734	165
对象	""bsnum""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
734.              String bsnum =
request.getParameter("bsnum")==null?"":request.getParameter("bsnum");
....
753.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
153.                    sb.append(" AND T.BSNUM LIKE
'"+CTools.escapeLike(bsnum)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3266:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3266
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	664	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
664.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
681.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3267:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3267
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	664	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String done(HttpServletRequest request,

```
....
664.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
681.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3268:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3268
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	699	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
699.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
716.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3269:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3269
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	699	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String temporary(HttpServletRequest request,

```
....
699.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
716.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3270:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3270
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	626	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
626.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
645.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3271:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3271
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	626	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String todo(HttpServletRequest request,

```
....
626.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
645.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3272:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3272
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	674	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
674.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
679.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3273:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3273
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	674	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String todo(HttpServletRequest request,

```
....
674.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
679.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),st
atus,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3274:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3274
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	706	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
706.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
709.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3275:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3275
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	706	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String done(HttpServletRequest request,

```
....
706.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
709.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3276:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3276
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	736	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
736.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3277:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3277
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	736	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String temporary(HttpServletRequest request,

```
....
736.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
739.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3278:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3278
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	767	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
767.              String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
770.              Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3279:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3279
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	767	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String back(HttpServletRequest request,

```
....
767.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
770.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3280:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3280
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	735	133
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
753.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
126.                    sbcount.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
129.              sbcount.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
....
131.              Query querycount =
getSession().createSQLQuery(sbcount.toString()).setString(0,
applicantid);
132.              querycount.setCacheable(false);
133.              List listcount = querycount.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.                int len = key.length();
....
815.                      char c = key.charAt(i);
....
830.                            buf.append(c);
....
827.                            buf.append("[%]");
....
824.                            buf.append("[_]");
....
821.                            buf.append("[[]");
....
818.                            buf.append("''");// 单引号替换成两个单引号
....
836.                return buf.toString();
```

SQL Injection\路径 3281:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3281
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	735	165
对象	""sxname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String back(HttpServletRequest request,

```
....
735.                String sxname =
request.getParameter("sxname")==null?"":request.getParameter("sxname");
....
753.                Pagination pagination =
enterpriseBanShiTingService.getPageForBanjian(user.getId().toString(),bj
status,cpn(pageNo),5,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
49.   public Pagination getPageForBanjian(String applicantid,String
status,int pageNo,int pageSize,String bsnum,String sxname){
50.         return
enterpriseBanShiTingDao.getPageForBanjian(applicantid,status,pageNo,page
Size,bsnum,sxname);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getPageForBanjian(String applicantid,String status,int pageNo,int pageSize,String bsnum,String sxname){

```
....
105.        public Pagination getPageForBanjian(String
applicantid,String status,int pageNo,int pageSize,String bsnum,String
sxname){
....
156.                    sb.append(" AND T.PNAME LIKE
'"+CTools.escapeLike(sxname)+"'");
....
158.              sb.append(" AND T.CREATETIME IS NOT NULL ORDER BY
T.CREATETIME DESC");
159.              sb.append(") tv)R WHERE R.RNUM>");
160.              sb.append((pageNo-1)*pageSize);
161.              sb.append(" AND R.RNUM<=");
162.              sb.append(pageNo*pageSize);
163.              Query query =
getSession().createSQLQuery(sb.toString()).setString(0, applicantid);
164.              query.setCacheable(false);
165.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key) {

```
....
791.        public static String escapeLike(String key) {
792.              return escapeLike(key, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String escapeLike(String key, boolean needPercent) {

```
....
802.        public static String escapeLike(String key, boolean
needPercent) {
....
812.              int len = key.length();
....
815.                    char c = key.charAt(i);
....
830.                          buf.append(c);
....
827.                          buf.append("[%]");
....
824.                          buf.append("[_]");
....
821.                          buf.append("[[]");
....
818.                          buf.append("''");// 单引号替换成两个单引号
....
836.              return buf.toString();
```

SQL Injection\路径 3282:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3282
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	552	241
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
552.              String name  = request.getParameter("selname");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.                if (baseString != null &&
baseString.trim().length()>0) {
710.                        char[] chars = baseString.toCharArray();
....
713.                              sb.append(chars[i] + addString);
....
715.                        return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
225.                countSql.append(name);
226.                countSql.append("%' AND T.AREAID='");
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

SQL Injection\路径 3283:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3283
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	552	474
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
552.              String name  = request.getParameter("selname");
....
572.              Map<String, Object>
deptServerMap=lawGuideMng.getServiceRegisterByName(com.jeecms.cms.CTools
.getStringAdd(name,"%"),areaid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.              if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                          sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
124.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
125.              return dao.getServiceRegisterByName(sxzxname,areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
466.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
....
469.                                "from v_t_share_permissionitem bean
where  bean.areaid=? and bean.sxzxname like '%"+sxzxname+"%'";
....
468.              String sql="select count(1) serverCount,COUNT(CASE
WHEN bean.SFWSSB = 1 THEN 1  ELSE  NULL  END)  as wssbCount " +
....
471.              SQLQuery query=this.getSession().createSQLQuery(sql);
472.              query.setString(0, areaId);
473.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
474.              List<Object> list=query.list();
```

SQL Injection\路径 3284:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3284
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	552	272
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
552.              String name  = request.getParameter("selname");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.                if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                        sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
254.                sb.append(name);
255.                sb.append("%' AND T.AREAID='");
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3285:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3285

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	590	218
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
590.              String name  = request.getParameter("selname");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.              if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                          sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
202.              countSql.append(name);
203.              countSql.append("%' AND T.AREAID='");
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

SQL Injection\路径 3286:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3286
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	590	474
对象	""selname""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String banshitingselpermissionitem(HttpServletRequest request,

```
....
590.              String name  = request.getParameter("selname");
....
610.              Map<String, Object>
deptServerMap=lawGuideMng.getServiceRegisterByName(com.jeecms.cms.CTools
.getStringAdd(name,"%"),areaid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java
方法	public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.                if (baseString != null &&
baseString.trim().length()>0) {
710.                        char[] chars = baseString.toCharArray();
....
713.                                sb.append(chars[i] + addString);
....
715.                        return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
124.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
125.                return dao.getServiceRegisterByName(sxzxname,areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public Map<String, Object> getServiceRegisterByName(String sxzxname,String areaId) {

```
....
466.        public Map<String, Object> getServiceRegisterByName(String
sxzxname,String areaId) {
....
469.                                "from v_t_share_permissionitem bean
where  bean.areaid=? and bean.sxzxname like '%"+sxzxname+"%'";
....
468.                String sql="select count(1) serverCount,COUNT(CASE
WHEN bean.SFWSSB = 1 THEN 1  ELSE  NULL  END)  as wssbCount " +
....
471.                SQLQuery query=this.getSession().createSQLQuery(sql);
472.                query.setString(0, areaId);
473.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
474.                List<Object> list=query.list();
```

SQL Injection\路径 3287:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3287
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	590	247
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
590.              String name  = request.getParameter("selname");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.              if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                          sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
230.                sb.append(name);
231.                sb.append("%' AND T.AREAID='");
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

SQL Injection\路径 3288:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3288
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	131	29
对象	""deptId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public void getPermissionitemByDeptId(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
131.                String deptid = request.getParameter("deptId");
....
134.                        list =
lawGuideMng.getPermissionitemForId(deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法	public List<VShowPermissionitem> getPermissionitemForId(String deptid) {

```
....
19.   public List<VShowPermissionitem> getPermissionitemForId(String
deptid) {
20.         return dao.getPermissionitemForId(deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
方法	public List<VShowPermissionitem> getPermissionitemForId(String deptid) {

```
....
25.   public List<VShowPermissionitem> getPermissionitemForId(String
deptid) {
26.         String hql = "from VShowPermissionitem t where t.deptid =
'"+deptid+"'";
27.         Query query = getSession().createQuery(hql);
28.         query.setCacheable(true);
29.         return query.list();
```

SQL Injection\路径 3289:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3289
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	128	29
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java
方法	public void getPermissionitemByDeptId(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
128.        public void getPermissionitemByDeptId(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
131.              String deptid = request.getParameter("deptId");
....
134.                    list =
lawGuideMng.getPermissionitemForId(deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java
方法	public List<VShowPermissionitem> getPermissionitemForId(String deptid) {

```
....
19.   public List<VShowPermissionitem> getPermissionitemForId(String
deptid) {
20.         return dao.getPermissionitemForId(deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
方法	public List<VShowPermissionitem> getPermissionitemForId(String deptid) {

```
....
25.   public List<VShowPermissionitem> getPermissionitemForId(String
deptid) {
26.         String hql = "from VShowPermissionitem t where t.deptid =
'"+deptid+"'";
27.         Query query = getSession().createQuery(hql);
28.         query.setCacheable(true);
29.         return query.list();
```

SQL Injection\路径 3290:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3290
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	287	36
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
287.              String name = request.getParameter("selname");
....
292.                    name = name.replaceAll("《", "");
293.                    name = name.replaceAll("》", "");
294.                    name = name.trim();
....
304.              List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptId,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 3291:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3291
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/cms/action/front/ZwgkAct.java	cms/cms/dao/main/impl/LawGuideDaoImpl.java
行	395	36
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduceList(String deptid, String permtype,

```
....
395.              String name = request.getParameter("selname");
....
399.                    name = name.replaceAll("《", "");
400.                    name = name.replaceAll("》", "");
401.                    name = name.trim();
....
411.              List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptid,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 3292:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3292

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	288	36
对象	""deptId""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
288.              String deptId = request.getParameter("deptId");
....
304.              List<TSharePermissionitem> listSP =
lawGuideMng.getPermissionitemForDeptId(deptId,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
23.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
24.         return dao.getPermissionitemForDeptId(deptid,fileName);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public List<TSharePermissionitem> getPermissionitemForDeptId(String deptid,String fileName){

```
....
32.   public List<TSharePermissionitem>
getPermissionitemForDeptId(String deptid,String fileName){
33.         String hql = "from TSharePermissionitem t where t.department
= '"+deptid+"' and t.forms like '%"+fileName+"%'";
34.         Query query = getSession().createQuery(hql);
35.         query.setCacheable(true);
36.         return query.list();
```

SQL Injection\路径 3293:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathi

	d=3293
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java
行	501	269
对象	""selname""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String selawproduce(HttpServletRequest request,

```
....
501.              String name = request.getParameter("selname");
....
506.                    name = name.replaceAll("《", "");
507.                    name = name.replaceAll("》", "");
508.                    name = name.trim();
....
536.              int
lawproduceCount=lawGuideMng.getLawproduceCount(com.jeecms.cms.CTools.get
StringAdd(name,"%"),deptid);//获取该部门下的事项总数和可网上办理事项总数
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/CTools.java

方法 public static String getStringAdd(String baseString, String addString) {

```
....
708.        public static String getStringAdd(String baseString, String
addString) {
709.              if (baseString != null &&
baseString.trim().length()>0) {
710.                    char[] chars = baseString.toCharArray();
....
713.                          sb.append(chars[i] + addString);
....
715.                    return sb.length() > 1 ? sb.substring(0,
sb.length() - 1) : sb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/LawGuideMngImpl.java

方法 public int getLawproduceCount(String name,String dept){

```
....
90.   public int getLawproduceCount(String name,String dept){
91.         return dao.getLawproduceCount(name,dept);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/LawGuideDaoImpl.java

方法 public int getLawproduceCount(String name,String dept) {

```
....
258.        public int getLawproduceCount(String name,String dept) {
....
261.              if(name != null && !name.equals("")){
262.                    sql += " and p.filename like '%"+name+"%' ";
....
266.              SQLQuery query=this.getSession().createSQLQuery(sql);
267.              query.setString(0, dept);
268.
      query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP);
269.              List<Object> list=query.list();
```

SQL Injection\路径 3294:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3294
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	369	87
对象	groupid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
375.                  xml = matterService.getClXml(sxid,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String sxid,String groupid) {

```
....
30.   public String getClXml(String sxid,String groupid) {
31.         String xml = this.matterDao.getClXml(sxid, groupid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXml(String sxid,String groupid) {

```
....
43.   public String getClXml(String sxid,String groupid) {
....
80.                                                 sql.append ( " and
t.groupid='"+groupid+"'");
....
82.                                                 sql.append( "and
t.sxid='"+sxid+"' )a \n" );
83.                                                 sql.append("  left join
T_END_SD_CLNR b on b.clid = a.id ");
....
87.         for(Object o:
getSession().createSQLQuery(sql.toString()).list()){
```

SQL Injection\路径 3295:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3295
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	369	87
对象	sxid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
375.                    xml = matterService.getClXml(sxid,groupid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getClXml(String sxid,String groupid) {

```
....
30.   public String getClXml(String sxid,String groupid) {
31.         String xml = this.matterDao.getClXml(sxid, groupid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXml(String sxid,String groupid) {

```
....
43.   public String getClXml(String sxid,String groupid) {
....
82.                                                 sql.append( "and
t.sxid='"+sxid+"' )a \n" );
83.                                                 sql.append("  left join
T_END_SD_CLNR b on b.clid = a.id ");
....
87.         for(Object o:
getSession().createSQLQuery(sql.toString()).list()){
```

SQL Injection\路径 3296:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3296
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	328	208
对象	sxid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
333.                        xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
204.              String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver from t_share_sxclgl t,t_share_clxx c
where c.id = t.clid and c.dzhyq='1' and t.changetype!='D' and t.sxid='"+
sxid + "'";
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3297:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3297
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	328	51
对象	sxid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
204.              String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver from t_share_sxclgl t,t_share_clxx c
where c.id = t.clid and c.dzhyq='1' and t.changetype!='D' and t.sxid='"+
sxid + "'";
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
209.              Object[] temp = (Object[]) o;
....
214.              xml.append("<xid>"+temp[3].toString()+"</xid>");
....
218.              xml.append("<formid>"+temp[3].toString()+"</formid>");
219.
      xml.append("<formver>"+temp[6].toString()+"</formver>");
....
236.              String html = getFormInfoHtmlData(sxid,
temp[3].toString(), temp[6].toString(),groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
440.        public String getFormInfoHtmlData(String sxid,String
formid,String formver,String groupid) {
....
443.                String sql02="from TXmlClob t where
t.formId='"+formid+"' and t.active='1'";
....
445.                List list = this.find(sql02);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3298:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3298
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	328	208
对象	groupid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
206.              sql += " and t.groupid='" + groupid + "'";
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3299:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3299
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	328	51

对象	groupid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
206.              sql += " and t.groupid='" + groupid + "'";
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
209.              Object[] temp = (Object[]) o;
....
214.              xml.append("<xid>"+temp[3].toString()+"</xid>");
....
218.              xml.append("<formid>"+temp[3].toString()+"</formid>");
219.
      xml.append("<formver>"+temp[6].toString()+"</formver>");
....
236.              String html = getFormInfoHtmlData(sxid,
temp[3].toString(), temp[6].toString(),groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
440.        public String getFormInfoHtmlData(String sxid,String
formid,String formver,String groupid) {
....
443.                String sql02="from TXmlClob t where
t.formId='"+formid+"' and t.active='1'";
....
445.                List list = this.find(sql02);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3300:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3300
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebAttcheClServiceImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	51	261
对象	sxid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebAttcheClServiceImpl.java
方法	public String queryCl(String bsnum,String sxid) {

```
....
51.   public String queryCl(String bsnum,String sxid) {
....
53.         String xml=matterDao.getClXmlForService(sxid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
260.              String sxNameSql = "select t.sxname from
t_share_permissionitem t where t.id='"+sxid+ "'";
261.              List
list=sessionFactory.openSession().createSQLQuery(sxNameSql).list();
```

SQL Injection\路径 3301:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3301
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebAttcheClServiceImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	51	271
对象	sxid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/WebAttcheClServiceImpl.java
方法	public String queryCl(String bsnum,String sxid) {

```
....
51.   public String queryCl(String bsnum,String sxid) {
....
53.         String xml=matterDao.getClXmlForService(sxid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
269.                            + sxid + "'";
....
268.              String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver,c.patterninstid
fid,c.orinum,c.copynum,c.clbh,t.sfby,c.bz,t.ordernum from t_share_sxclgl
t,t_share_clxx c where c.id = t.clid and c.dzhyq<>'1' and (t.changetype
is null or t.changetype = 'C' or t.changetype = 'U') and t.sxid='"
....
271.              for (Object o
:sessionFactory.openSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3302:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3302
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	46	261
对象	name	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java
方法	public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.               return request.getParameter(name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java
方法	public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.                 String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
260.                String sxNameSql = "select t.sxname from
t_share_permissionitem t where t.id='"+sxid+ "'";
261.                List
list=sessionFactory.openSession().createSQLQuery(sxNameSql).list();
```

SQL Injection\路径 3303:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3303
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	46	271
对象	name	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.                 return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.                 String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
269.                            + sxid + "'";
....
268.                String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver,c.patterninstid
fid,c.orinum,c.copynum,c.clbh,t.sfby,c.bz,t.ordernum from t_share_sxclgl
t,t_share_clxx c where c.id = t.clid and c.dzhyq<>'1' and (t.changetype
is null or t.changetype = 'C' or t.changetype = 'U') and t.sxid='"
....
271.                for (Object o
:sessionFactory.openSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3304:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3304
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	48	261
对象	getQueryString	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java
方法	public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
140.                    if (ht.containsKey(key)) {
141.                          String oldVals[] = (String[]) ht.get(key);
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java

方法 public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.               String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
260.              String sxNameSql = "select t.sxname from
t_share_permissionitem t where t.id='"+sxid+ "'";
261.              List
list=sessionFactory.openSession().createSQLQuery(sxNameSql).list();
```

SQL Injection\路径 3305:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3305
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	48	271
对象	getQueryString	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
140.                    if (ht.containsKey(key)) {
141.                          String oldVals[] = (String[]) ht.get(key);
....
153.              return ht;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MobileScanAct.java
方法	public String getclInfo(HttpServletRequest request, ModelMap model) {

```
....
50.         String sxid = RequestUtils.getQueryParam(request, "sxid");
....
55.                 String returnxmlInfo =
matterDao.getClXmlForService(sxid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXmlForService(String sxid) {

```
....
255.        public String getClXmlForService(String sxid) {
....
269.                            + sxid + "'";
....
268.                String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver,c.patterninstid
fid,c.orinum,c.copynum,c.clbh,t.sfby,c.bz,t.ordernum from t_share_sxclgl
t,t_share_clxx c where c.id = t.clid and c.dzhyq<>'1' and (t.changetype
is null or t.changetype = 'C' or t.changetype = 'U') and t.sxid='"
....
271.                for (Object o
:sessionFactory.openSession().createSQLQuery(sql).list()) {
```

SQL Injection\路径 3306:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3306
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	369	511
对象	bsid	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
377.                    xml = matterService.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
36.   public String getClXml(String bsid) throws Exception{
37.         String xml = this.matterDao.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
467.        public String getClXml(String bsid) throws Exception{
....
496.              sql.append(" where t.ywid = '"+bsid+"') c\n" );
497.              sql.append("  left join T_END_SD_CLNR b on c.clid =
b.clid" );
....
511.              for(Object
sb:this.getSession().createSQLQuery(sql.toString()).list()){
```

SQL Injection\路径 3307:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3307
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	369	570
对象	bsid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
377.                    xml = matterService.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
36.   public String getClXml(String bsid) throws Exception{
37.         String xml = this.matterDao.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
467.        public String getClXml(String bsid) throws Exception{
....
496.              sql.append(" where t.ywid = '"+bsid+"') c\n" );
497.              sql.append("  left join T_END_SD_CLNR b on c.clid =
b.clid" );
....
511.              for(Object
sb:this.getSession().createSQLQuery(sql.toString()).list()){
....
524.
      xml.append("<gid>"+changeStr(temp[3].toString())+"</gid>");
....
540.
      xml.append("<uid>"+changeStr(temp[6].toString())+"</uid>");
....
550.                          if(null !=
element.element("materialname").getText() &&
element.element("materialname").getText().equals(temp[1].toString())){
....
569.                                  String sql2 = "select t.sfby from
t_share_sxclgl t where t.clid = '"+temp[0].toString()+"' and
t.sxid='"+sxid+"'";
570.                                  List list =
getSession().createSQLQuery(sql2).list();
```

SQL Injection\路径 3308:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3308
结果评论
被分配给

状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	369	51
对象	bsid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
377.                    xml = matterService.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
36.   public String getClXml(String bsid) throws Exception{
37.         String xml = this.matterDao.getClXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
467.        public String getClXml(String bsid) throws Exception{
....
502.              TInsWebhallBusinessInfo info =
(TInsWebhallBusinessInfo)this.getSession().get(TInsWebhallBusinessInfo.c
lass, bsid);
....
504.              String sql01="from TSharePermissionitem t where
t.sxbh='"+info.getPid()+"' and t.sxzxbh = '"+info.getItemid()+"'";
505.              List<TSharePermissionitem> ps = this.find(sql01);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsWebhallBusinessInfo.java

方法 public String getItemid() {

```
....
128.              return itemid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.           return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3309:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3309
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	307	764
对象	sxid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
312.                    xml =
matterService.getFormInfoXml(sxid,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
41.   public String getFormInfoXml(String sxid, String groupid) {
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
660.        public String getFormInfoXml(String sxid, String groupid) {
....
760.              String sql = "select c.id,c.clmc,c.dzhyq,c.xmlid,''
gid,t.baseinfo baseinfo,c.formver from t_share_sxclgl t,t_share_clxx c
where c.id = t.clid and c.dzhyq='1' and t.sxid='"+sxid+"'";
....
764.              for(Object o:
this.getSession().createSQLQuery(sql).list()){
```

SQL Injection\路径 3310:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3310
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	307	51
对象	sxid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
312.                    xml =
matterService.getFormInfoXml(sxid,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
41.   public String getFormInfoXml(String sxid, String groupid) {
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
660.        public String getFormInfoXml(String sxid, String groupid) {
....
664.              String sql01="from TSysFlowlibmapform t where
t.sxid='"+sxid+"' ";
665.              List<TSysFlowlibmapform> performlist=this.find(sql01);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3311:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3311
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	307	764
对象	groupid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
312.                    xml =
matterService.getFormInfoXml(sxid,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
41.   public String getFormInfoXml(String sxid, String groupid) {
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
660.        public String getFormInfoXml(String sxid, String groupid) {
....
762.                    sql += " and t.groupid='"+groupid+"'";
....
764.              for(Object o:
this.getSession().createSQLQuery(sql).list()){
```

SQL Injection\路径 3312:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3312
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	291	880
对象	sxid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String clxxgroup(String sxid, HttpServletRequest request,

```
....
291.        public String clxxgroup(String sxid, HttpServletRequest
request,
....
295.                    String xml=matterService.getGroupXml(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getGroupXml(String sxid) throws Exception {

```
....
64.   public String getGroupXml(String sxid) throws Exception {
65.         String xml = this.matterDao.getGroupXml(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getGroupXml(String sxid) throws Exception {

```
....
874.        public String getGroupXml(String sxid) throws Exception {
....
877.                String sql = "select distinct
g.p_group_id,g.p_group_name from t_share_sxclgl s,t_share_clxx_group g
where s.groupid = g.p_group_id and g.changetype!='D' and
s.sxid='"+sxid+"'";
....
880.                for(Object o:
this.getSession().createSQLQuery(sql).list()){
```

SQL Injection\路径 3313:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3313
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
行	125	175
对象	""sxbh""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String sxinfo(HttpServletRequest request,

```
....
125.                String sxbh = request.getParameter("sxbh");
126.                List  list
=permissionMng.getPermissionitemForSxbhqb(deptId, sxbh.substring(0,
sxbh.length()-1));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法 public List getPermissionitemForSxbhqb(String deptid,

```
....
49.                 String sxbh) {
50.         return dao.getPermissionitemForSxbhqb(deptid,sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java

方法 public List getPermissionitemForSxbhqb(String deptid,String sxbh) {

```
....
164.        public List getPermissionitemForSxbhqb(String deptid,String
sxbh) {
....
169.              String sql ="SELECT T.ID SXID, T.SXBH, DECODE(T.XZXK,
'1', '行政许可事项',  '2', '非行政许可审批事项', '3', '社会事务服务事项',
'社会事务服务事项') XZXKNAME, T.SXZXNAME, (SELECT COUNT(1) FROM
T_SHARE_PERMISSIONITEM WHERE SXBH = T.SXBH AND T.DEPARTMENT =
DEPARTMENT) ISSXBH,T.SXZXBH, T.SXNAME,  T.XZXK, T2.DEPTID, T3.AREAID
FROM T_SHARE_PERMISSIONITEM T INNER JOIN T_SYS_DEPT T2 ON T.DEPARTMENT =
T2.DEPTID INNER JOIN T_SYS_REGION T3 ON T2.AREAID = T3.AREAID LEFT JOIN
T_SHARE_WEBCONDITION T4 ON T.ID = T4.PERMID AND T4.CHANGETYPE != 'D'
WHERE T.STATUS = '1' AND T2.TYPE = '0' AND t2.deptid='"+deptid+"' AND
t.sxbh IN("+sxbh+") ORDER BY T2.ORDERID || '-' || T.SXBH || '-' ||
T.SXZXBH";
170.              Query query = getSession().createSQLQuery(sql);
....
175.              List ob = query.list();
```

SQL Injection\路径 3314:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3314
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
行	120	175
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String sxinfo(HttpServletRequest request,

```
....
120.        public String sxinfo( HttpServletRequest request,
....
124.              String deptId = request.getParameter("deptId");
125.              String sxbh = request.getParameter("sxbh");
126.              List  list
=permissionMng.getPermissionitemForSxbhqb(deptId, sxbh.substring(0,
sxbh.length()-1));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法	public List getPermissionitemForSxbhqb(String deptid,

```
....
49.                 String sxbh) {
50.         return dao.getPermissionitemForSxbhqb(deptid,sxbh);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
方法	public List getPermissionitemForSxbhqb(String deptid,String sxbh) {

```
....
164.        public List getPermissionitemForSxbhqb(String deptid,String
sxbh) {
....
169.                String sql ="SELECT T.ID SXID, T.SXBH, DECODE(T.XZXK,
'1', '行政许可事项',  '2', '非行政许可审批事项', '3', '社会事务服务事项',
'社会事务服务事项') XZXKNAME, T.SXZXNAME, (SELECT COUNT(1) FROM
T_SHARE_PERMISSIONITEM WHERE SXBH = T.SXBH AND T.DEPARTMENT =
DEPARTMENT) ISSXBH,T.SXZXBH, T.SXNAME,  T.XZXK, T2.DEPTID, T3.AREAID
FROM T_SHARE_PERMISSIONITEM T INNER JOIN T_SYS_DEPT T2 ON T.DEPARTMENT =
T2.DEPTID INNER JOIN T_SYS_REGION T3 ON T2.AREAID = T3.AREAID LEFT JOIN
T_SHARE_WEBCONDITION T4 ON T.ID = T4.PERMID AND T4.CHANGETYPE != 'D'
WHERE T.STATUS = '1' AND T2.TYPE = '0' AND t2.deptid='"+deptid+"' AND
t.sxbh IN("+sxbh+") ORDER BY T2.ORDERID || '-' || T.SXBH || '-' ||
T.SXZXBH";
170.                Query query = getSession().createSQLQuery(sql);
....
175.                List ob = query.list();
```

SQL Injection\路径 3315:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3315
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
行	124	175
对象	""deptId""	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java
方法	public String sxinfo(HttpServletRequest request,

```
....
124.              String deptId = request.getParameter("deptId");
....
126.              List  list
=permissionMng.getPermissionitemForSxbhqb(deptId, sxbh.substring(0,
sxbh.length()-1));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法 public List getPermissionitemForSxbhqb(String deptid,

```
....
48.   public List getPermissionitemForSxbhqb(String deptid,
....
50.         return dao.getPermissionitemForSxbhqb(deptid,sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java

方法 public List getPermissionitemForSxbhqb(String deptid,String sxbh) {

```
....
164.        public List getPermissionitemForSxbhqb(String deptid,String
sxbh) {
....
169.              String sql ="SELECT T.ID SXID, T.SXBH, DECODE(T.XZXK,
'1', '行政许可事项',  '2', '非行政许可审批事项', '3', '社会事务服务事项',
'社会事务服务事项') XZXKNAME, T.SXZXNAME, (SELECT COUNT(1) FROM
T_SHARE_PERMISSIONITEM WHERE SXBH = T.SXBH AND T.DEPARTMENT =
DEPARTMENT) ISSXBH,T.SXZXBH, T.SXNAME,  T.XZXK, T2.DEPTID, T3.AREAID
FROM T_SHARE_PERMISSIONITEM T INNER JOIN T_SYS_DEPT T2 ON T.DEPARTMENT =
T2.DEPTID INNER JOIN T_SYS_REGION T3 ON T2.AREAID = T3.AREAID LEFT JOIN
T_SHARE_WEBCONDITION T4 ON T.ID = T4.PERMID AND T4.CHANGETYPE != 'D'
WHERE T.STATUS = '1' AND T2.TYPE = '0' AND t2.deptid='"+deptid+"' AND
t.sxbh IN("+sxbh+") ORDER BY T2.ORDERID || '-' || T.SXBH || '-' ||
T.SXZXBH";
170.              Query query = getSession().createSQLQuery(sql);
....
175.              List ob = query.list();
```

SQL Injection\路径 3316:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3316
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/cms/action/front/LawGuideAct.java	cms/cms/dao/main/impl/PermissionDaoImpl.java
行	129	217
对象	""sortCode""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawGuideInfo(HttpServletRequest request,

```
....
129.              String sortCode = request.getParameter("sortCode");
....
131.              List  list
=permissionMng.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法 public List getPermissionitemSortForSxbhTwo(

```
....
68.               String sortCode, String sxbh) {
....
70.         return dao.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java

方法 public List getPermissionitemSortForSxbhTwo(String sortCode,String sxbh) {

```
....
182.        public List getPermissionitemSortForSxbhTwo(String
sortCode,String sxbh) {
....
186.              if(sortCode!=null && !sortCode.equals("")){
....
188.                    String[] scode = sortCode.split(",");
....
195.                                sql.append("'"+scode[i]+"'");
....
192.                                sql.append("'"+scode[i]+"',");
....
198.                    sql.append(") ");
....
214.              sql.append(" order by p.id");
215.              Query query =
getSession().createSQLQuery(sql.toString());
216.              System.out.println(query.getQueryString());
217.              return query.list();
```

SQL Injection\路径 3317:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3317
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
行	127	217
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawGuideInfo(HttpServletRequest request,

```
....
127.        public String lawGuideInfo( HttpServletRequest request,
....
129.                String sortCode = request.getParameter("sortCode");
....
131.                List  list
=permissionMng.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法 public List getPermissionitemSortForSxbhTwo(

```
....
68.                 String sortCode, String sxbh) {
....
70.         return dao.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java

方法 public List getPermissionitemSortForSxbhTwo(String sortCode,String sxbh) {

```
....
182.        public List getPermissionitemSortForSxbhTwo(String
sortCode,String sxbh) {
....
186.              if(sortCode!=null && !sortCode.equals("")){
....
188.                    String[] scode = sortCode.split(",");
....
195.                                sql.append("'"+scode[i]+"'");
....
192.                                sql.append("'"+scode[i]+"',");
....
198.                    sql.append(") ");
....
214.              sql.append(" order by p.id");
215.              Query query =
getSession().createSQLQuery(sql.toString());
216.              System.out.println(query.getQueryString());
217.              return query.list();
```

SQL Injection\路径 3318:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3318
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
行	130	217
对象	""sxbh""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String lawGuideInfo(HttpServletRequest request,

```
....
130.              String sxbh = request.getParameter("sxbh");
131.              List  list
=permissionMng.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/PermissionMngImpl.java

方法 public List getPermissionitemSortForSxbhTwo(

```
....
68.               String sortCode, String sxbh) {
....
70.         return dao.getPermissionitemSortForSxbhTwo(sortCode, sxbh);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/PermissionDaoImpl.java
方法	public List getPermissionitemSortForSxbhTwo(String sortCode,String sxbh) {

```
....
182.        public List getPermissionitemSortForSxbhTwo(String
sortCode,String sxbh) {
....
202.              if(sxbh != null && !sxbh.equals("")){
203.                    String[] sx = sxbh.split(",");
....
209.                                 sql.append("'"+sx[j]+"'");
....
207.                                 sql.append("'"+sx[j]+"',");
....
212.                    sql.append(")");
....
214.              sql.append(" order by p.id");
215.              Query query =
getSession().createSQLQuery(sql.toString());
216.              System.out.println(query.getQueryString());
217.              return query.list();
```

SQL Injection\路径 3319:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3319
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java
行	155	37
对象	""deptId""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java
方法	public void getTimeperiodByDate(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
155.              String deptid = request.getParameter("deptId");
....
159.                      map =
reservationMng.getTimeperiodByDate(time,deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ReservationMngImpl.java

方法 public Map getTimeperiodByDate(String createtime,String deptid) {

```
....
37.   public Map getTimeperiodByDate(String createtime,String deptid) {
....
39.         List list = this.dao.getTimeperiodByDate(createtime,deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java

方法 public List getTimeperiodByDate(String createtime,String deptid) {

```
....
34.   public List getTimeperiodByDate(String createtime,String deptid) {
....
36.                " where t.lasttime = '"+createtime+"' and  t.deptid =
'"+deptid+"'"+
....
35.         return getSession().createSQLQuery("select t.advice,
count(1) total from t_ins_webhall_business t "+
....
37.                " group by t.advice ").list();
```

SQL Injection\路径 3320:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3320
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java
行	151	37
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java
方法	public void getTimeperiodByDate(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
151.        public void getTimeperiodByDate(HttpServletRequest
request,HttpServletResponse response, ModelMap model){
....
154.              String time = request.getParameter("createdate");
155.              String deptid = request.getParameter("deptId");
....
159.                    map =
reservationMng.getTimeperiodByDate(time,deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ReservationMngImpl.java
方法	public Map getTimeperiodByDate(String createtime,String deptid) {

```
....
37.   public Map getTimeperiodByDate(String createtime,String deptid) {
....
39.         List list = this.dao.getTimeperiodByDate(createtime,deptid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java
方法	public List getTimeperiodByDate(String createtime,String deptid) {

```
....
34.   public List getTimeperiodByDate(String createtime,String deptid) {
....
36.                " where t.lasttime = '"+createtime+"' and  t.deptid =
'"+deptid+"'"+
....
35.         return getSession().createSQLQuery("select t.advice,
count(1) total from t_ins_webhall_business t "+
....
37.                " group by t.advice ").list();
```

SQL Injection\路径 3321:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3321
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/cms/action/member/ReservationAct.java	cms/cms/dao/main/impl/ReservationDaoImpl.java
行	154	37
对象	""createdate""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ReservationAct.java

方法 public void getTimeperiodByDate(HttpServletRequest request,HttpServletResponse response, ModelMap model){

```
....
154.              String time = request.getParameter("createdate");
....
159.                    map =
reservationMng.getTimeperiodByDate(time,deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ReservationMngImpl.java

方法 public Map getTimeperiodByDate(String createtime,String deptid) {

```
....
37.   public Map getTimeperiodByDate(String createtime,String deptid) {
....
39.         List list = this.dao.getTimeperiodByDate(createtime,deptid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/ReservationDaoImpl.java

方法 public List getTimeperiodByDate(String createtime,String deptid) {

```
....
34.   public List getTimeperiodByDate(String createtime,String deptid) {
....
36.                " where t.lasttime = '"+createtime+"' and  t.deptid =
'"+deptid+"'"+
....
35.         return getSession().createSQLQuery("select t.advice,
count(1) total from t_ins_webhall_business t "+
....
37.                " group by t.advice ").list();
```

SQL Injection\路径 3322:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3322

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	1035	108
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法 public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1035.                    public String exportAll(String id,
HttpServletRequest request,HttpServletResponse response,
....
1040.                                        id=request.getParameter("id");
....
1042.                                        CmsSite site =
CmsUtils.getSite(request);
1043.                                        List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
67.   public static CmsSite getSite(HttpServletRequest request) {
68.          return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java

方法 public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.          return dao.getList(site, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java

方法 public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.             Query query = getSession().createQuery(hql);
107.             query.setCacheable(cacheable);
108.             return query.list();
```

SQL Injection\路径 3323:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3323
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java
行	97	47
对象	""bid""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public void preCounsel2(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
97.         String bid = request.getParameter("bid");
....
107.             VTInsBusinessinfo info =
businessTagMng.findByIdAndName(bid.trim(), bsrname.trim());
....
110.                    List<TInsAdvice> list =
this.tInsAdviceService.findByBsnum(bid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsAdviceServiceImpl.java

方法 public List<TInsAdvice> findByBsnum(String bsnum){

```
....
34.   public List<TInsAdvice> findByBsnum(String bsnum){
35.         return this.dao.findByBsnum(bsnum);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java
方法	public List<TInsAdvice> findByBsnum(String bsnum){

```
....
44.   public List<TInsAdvice> findByBsnum(String bsnum){
45.         String hql = "from TInsAdvice t where 1=1 and
t.bsnum='"+bsnum+"' ";
46.         Query query = getSession().createQuery(hql);
47.         return query.list();
```

SQL Injection\路径 3324:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3324
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java
行	95	47
对象	request	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java
方法	public void preCounsel2(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
95.   public void preCounsel2(HttpServletRequest
request,HttpServletResponse response, ModelMap model) throws Exception {
....
97.         String bid = request.getParameter("bid");
....
107.              VTInsBusinessinfo info =
businessTagMng.findByIdAndName(bid.trim(), bsrname.trim());
....
110.                    List<TInsAdvice> list =
this.tInsAdviceService.findByBsnum(bid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsAdviceServiceImpl.java
方法	public List<TInsAdvice> findByBsnum(String bsnum){

```
....
34.   public List<TInsAdvice> findByBsnum(String bsnum){
35.         return this.dao.findByBsnum(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java

方法 public List<TInsAdvice> findByBsnum(String bsnum){

```
....
44.   public List<TInsAdvice> findByBsnum(String bsnum){
45.         String hql = "from TInsAdvice t where 1=1 and
t.bsnum='"+bsnum+"' ";
46.         Query query = getSession().createQuery(hql);
47.         return query.list();
```

SQL Injection\路径 3325:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3325
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImpl.java
行	49	30
对象	id	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxAct.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
49.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
57.         TTyspGrsbclxx twebhallGrsbClxx =
twebhallGrsbClxxService.getTTyspGrsbclxxById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallGrsbClxxMngImpl.java

方法 public TTyspGrsbclxx getTTyspGrsbclxxById(String id) {

```
....
22.   public TTyspGrsbclxx getTTyspGrsbclxxById(String id) {
23.         return dao.getTTyspGrsbclxxById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImpl.java

方法 public TTyspGrsbclxx getTTyspGrsbclxxById(String id){

```
....
25.   public TTyspGrsbclxx getTTyspGrsbclxxById(String id){
26.         String hql = "from TTyspGrsbclxx t where t.id = '"+id+"'";
27.         Query query = getSession().createQuery(hql);
28.         query.setCacheable(true);
....
30.         List<TTyspGrsbclxx> list = query.list();
```

SQL Injection\路径 3326:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3326
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImplgr.java
行	48	30
对象	id	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/TWebhallGrsbClxxActgr.java

方法 public String lawguide(@PathVariable String id, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String id, HttpServletRequest
request,
....
56.         TTyspGrsbclxx twebhallGrsbClxx =
twebhallGrsbClxxServicegr.getTTyspGrsbclxxById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallGrsbClxxMngImplgr.java

方法 public TTyspGrsbclxx getTTyspGrsbclxxById(String id) {

```
....
25.   public TTyspGrsbclxx getTTyspGrsbclxxById(String id) {
26.         return dao.getTTyspGrsbclxxById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallGrsbClxxDaoImplgr.java

方法 public TTyspGrsbclxx getTTyspGrsbclxxById(String id){

```
....
25.   public TTyspGrsbclxx getTTyspGrsbclxxById(String id){
26.         String hql = "from TTyspGrsbclxx t where t.id = '"+id+"'";
27.         Query query = getSession().createQuery(hql);
28.         query.setCacheable(true);
....
30.         List<TTyspGrsbclxx> list = query.list();
```

SQL Injection\路径 3327:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3327
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinessDaoImpl.java
行	272	154
对象	deptName	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java

方法 public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
294.              Pagination p =
webhallBusinessMng.getBusinessCouncilList(deptName, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebhallBusinessMngImpl.java

方法	public Pagination getBusinessCouncilList(String deptname,int pageNo,int pageSize){

```
....
44.   public Pagination getBusinessCouncilList(String deptname,int
pageNo,int pageSize){
45.         return this.dao.getPageForBusinessCouncil(deptname, pageNo,
pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinesDaoImpl.java
方法	public Pagination getPageForBusinessCouncil(String deptName,int pageNo,int pageSize){

```
....
139.        public Pagination getPageForBusinessCouncil(String
deptName,int pageNo,int pageSize){
....
147.                    hql += "and VTIW.deptname like'%" + deptName +
"%'";
....
153.              Query query = getSession().createQuery(hql);
154.              List<Object[]> listo = query.list();
```

SQL Injection\路径 3328:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3328
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinessAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinesDaoImpl.java
行	272	165
对象	deptName	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebhallBusinesAct.java
方法	public String bussinessCouncilList(String deptName,Integer pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {

```
....
272.        public String bussinessCouncilList(String deptName,Integer
pageNo,Integer pageSize, HttpServletRequest request, ModelMap model) {
....
294.              Pagination p =
webhallBusinessMng.getBusinessCouncilList(deptName, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebhallBusinessMngImpl.java

方法 public Pagination getBusinessCouncilList(String deptname,int pageNo,int pageSize){

```
....
44.   public Pagination getBusinessCouncilList(String deptname,int
pageNo,int pageSize){
45.         return this.dao.getPageForBusinessCouncil(deptname, pageNo,
pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinesDaoImpl.java

方法 public Pagination getPageForBusinessCouncil(String deptName,int pageNo,int pageSize){

```
....
139.        public Pagination getPageForBusinessCouncil(String
deptName,int pageNo,int pageSize){
....
147.                    hql += "and VTIW.deptname like'%" + deptName +
"%'";
....
153.              Query query = getSession().createQuery(hql);
154.              List<Object[]> listo = query.list();
....
163.              query.setFirstResult(p.getFirstResult());
164.              query.setMaxResults(p.getPageSize());
165.              listo = query.list();
```

SQL Injection\路径 3329:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3329
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

行	59	32
对象	reminderCode	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
59.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
67.         WebpageFavorite WebpageFavorite =
WebpageFavoriteMng.getWebpageFavoriteById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public WebpageFavorite getWebpageFavoriteById(String favoriteCode) {

```
....
38.   public WebpageFavorite getWebpageFavoriteById(String favoriteCode)
{
....
40.         return
WebpageFavoriteDao.getWebpageFavoriteById(favoriteCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public WebpageFavorite getWebpageFavoriteById(String favoriteCode){

```
....
27.   public WebpageFavorite getWebpageFavoriteById(String
favoriteCode){
28.         String hql = "from WebpageFavorite t where t.favoriteCode =
'"+favoriteCode+"'";
29.         Query query = getSession().createQuery(hql);
30.         query.setCacheable(true);
....
32.         List<WebpageFavorite> list = query.list();
```

SQL Injection\路径 3330:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3330

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java
行	54	31
对象	reminderCode	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
54.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
62.         WebpageFavoritegr WebpageFavoritegr =
WebpageFavoriteMnggr.getWebpageFavoritegrById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java

方法 public WebpageFavoritegr getWebpageFavoritegrById(String favoriteCode) {

```
....
29.   public WebpageFavoritegr getWebpageFavoritegrById(String
favoriteCode) {
....
31.         return
WebpageFavoriteDaogr.getWebpageFavoritegrById(favoriteCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java

方法 public WebpageFavoritegr getWebpageFavoritegrById(String favoriteCode){

```
....
26.   public WebpageFavoritegr getWebpageFavoritegrById(String
favoriteCode){
27.         String hql = "from WebpageFavoritegr t where t.favoriteCode
= '"+favoriteCode+"'";
28.         Query query = getSession().createQuery(hql);
29.         query.setCacheable(true);
....
31.         List<WebpageFavoritegr> list = query.list();
```

SQL Injection\路径 3331:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathi

	d=3331
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImpl.java
行	48	31
对象	reminderCode	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderAct.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
56.         WebpageReminder webpageReminder =
webpageReminderMng.getWebpageReminderById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageReminderMngImpl.java

方法 public WebpageReminder getWebpageReminderById(String reminderCode) {

```
....
26.   public WebpageReminder getWebpageReminderById(String reminderCode)
{
....
28.         return dao.getWebpageReminderById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImpl.java

方法 public WebpageReminder getWebpageReminderById(String reminderCode){

```
....
26.   public WebpageReminder getWebpageReminderById(String
reminderCode){
27.         String hql = "from WebpageReminder t where t.reminderCode =
'"+reminderCode+"'";
28.         Query query = getSession().createQuery(hql);
29.         query.setCacheable(true);
....
31.         List<WebpageReminder> list = query.list();
```

SQL Injection\路径 3332:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3332
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImplgr.java
行	48	31
对象	reminderCode	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageReminderActgr.java

方法 public String lawguide(@PathVariable String reminderCode, HttpServletRequest request,

```
....
48.   public String lawguide(@PathVariable String reminderCode,
HttpServletRequest request,
....
56.         WebpageRemindergr webpageReminder =
webpageReminderMnggr.getWebpageRemindergrById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageReminderMngImplgr.java

方法 public WebpageRemindergr getWebpageRemindergrById(String reminderCode) {

```
....
29.   public WebpageRemindergr getWebpageRemindergrById(String
reminderCode) {
....
31.         return dao.getWebpageRemindergrById(reminderCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageReminderDaoImplgr.java

方法 public WebpageRemindergr getWebpageRemindergrById(String reminderCode){

```
....
26.   public WebpageRemindergr getWebpageRemindergrById(String
reminderCode){
27.         String hql = "from WebpageRemindergr t where t.reminderCode
= '"+reminderCode+"'";
28.         Query query = getSession().createQuery(hql);
29.         query.setCacheable(true);
....
31.         List<WebpageRemindergr> list = query.list();
```

SQL Injection\路径 3333:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3333
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java
行	713	141
对象	cllist	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String sbsubmit(String cllist,String formlist,String poststr, HttpServletRequest request,

```
....
713.        public String sbsubmit(String cllist,String formlist,String
poststr, HttpServletRequest request,
....
751.              String sqpz_xml=wssbService.saveOrUpdate(cllist,
flist, AREAID ,request);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String saveOrUpdate(String xmlStr,

```
....
117.        public String saveOrUpdate(String xmlStr,
....
144.                          dataxml=ywpzGenerator(insbusi, xmlStr
,request.getParameter("promise_value"));// 0708注销
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 private String ywpzGenerator(TInsWebhallBusinessInfo insbusi, String xmlStr,String promise_value)

```
....
514.        private String ywpzGenerator(TInsWebhallBusinessInfo
insbusi, String xmlStr,String promise_value)
....
518.              StringReader reader = new StringReader(xmlStr);
519.              InputSource source = new InputSource(reader);
520.              org.w3c.dom.Document document = db.parse(source);
521.              NodeList cNodeList =
document.getElementsByTagName("cl");
....
549.                    for (int i = 0; i < cNodeList.getLength(); i++)
{
550.                          org.w3c.dom.Element dataNode =
(org.w3c.dom.Element) cNodeList.item(i);
551.                          String no =
dataNode.getAttributes().getNamedItem("no").getNodeValue();
552.                          String clmc =
dataNode.getAttributes().getNamedItem("clmc").getNodeValue();
....
554.                          String clid =
dataNode.getAttributes().getNamedItem("clid").getNodeValue();// 材料
555.                          String clbz = this.getClBz(clid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getClBz(String clid) {

```
....
705.        public String getClBz(String clid) {
706.              return wssbDao.getClBzInfo(clid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public String getClBzInfo(String clid){

```
....
133.      public String getClBzInfo(String clid){
....
136.            hql += " and t.id = '" + clid + "'";
....
138.        Query query = this.getSession().createQuery(hql);
....
141.              clbz = query.list().get(0).toString();
```

SQL Injection\路径 3334:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathi

	d=3334
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TShareServiceImpl.java
行	170	72
对象	""sxid""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java

方法 public void doPost(HttpServletRequest request, HttpServletResponse response)

```
....
170.                    String sxid = request.getParameter("sxid");
....
383.                                        List rsl =
tShareService.getDirForUpload(sxid);// 文件夹
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TShareServiceImpl.java

方法 public List<String> getDirForUpload(String sxid){

```
....
62.    public List<String> getDirForUpload(String sxid){
....
68.                sql += "and per.id = '"+sxid+"'";
....
72.                    List iterate =
session.createSQLQuery(sql).list();
```

SQL Injection\路径 3335:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3335
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

行	220	51
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseAct.java

方法 public String index2(String areaId, String stab,

```
....
220.        public String index2(String areaId, String stab,
....
247.                    if(areaId.length()>6){
248.                        areaId = areaId.substring(0,6);
....
251.                                .getListByParentId(areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListByParentId(String parentid) {

```
....
29.   public List<SysRegion> getListByParentId(String parentid) {
30.         return dao.getListByParentId(parentid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getListByParentId(String parentid) {

```
....
37.   public List<SysRegion> getListByParentId(String parentid) {
38.         String hql = "from SysRegion r where r.parentid =
'"+parentid+"' and r.status='1' order by r.areaid asc";
39.         return find(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3336:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3336
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	222	51
对象	areaId	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseActgr.java

方法 public String index2(String areaId, String stab,

```
....
222.        public String index2(String areaId, String stab,
....
246.                    if(areaId.length()>6){
247.                        areaId = areaId.substring(0,6);
....
250.                                    .getListByParentId(areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListByParentId(String parentid) {

```
....
29.   public List<SysRegion> getListByParentId(String parentid) {
30.         return dao.getListByParentId(parentid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java
方法	public List<SysRegion> getListByParentId(String parentid) {

```
....
37.   public List<SysRegion> getListByParentId(String parentid) {
38.         String hql = "from SysRegion r where r.parentid =
'"+parentid+"' and r.status='1' order by r.areaid asc";
39.         return find(hql);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3337:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3337
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	97	51
对象	qymc	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String mcchaxun(String qymc,Integer pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap model) {

```
....
97.   public String mcchaxun(String qymc,Integer
pageNo,HttpServletRequest request, HttpServletResponse response,ModelMap
model) {
....
107.              if (qymc != null&&!qymc.equals("")) {
....
111.                           List list = service.findByHQL("from
ExGongshang01Qymccxxx where qymc = '"+qymc+"' ");
112.                           if(list.size()!=0)
....
114.                                ExGongshang01Qymccxxx xx =
(ExGongshang01Qymccxxx)list.get(0);
115.                                String qyzch = xx.getQyzch();
116.                                List<GongShangweifa> list2 =
gongshangweifaTagMng.findByDwzzbh(qyzch);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/ExGongshang01Qymccxxx.java

方法 public String getQyzch() {

```
....
321.              return qyzch;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/GongShangweifaTagMngImpl.java

方法 public List<GongShangweifa> findByDwzzbh(String qyzch) {

```
....
28.   public List<GongShangweifa> findByDwzzbh(String qyzch) {
29.         return dao.findByDwzzbh(qyzch);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/gongshangwebservice/qymccx/impl/GongShangweifaTagDaoImpl.java

方法 public List<GongShangweifa> findByDwzzbh(String qyzch) {

```
....
35.   public List<GongShangweifa> findByDwzzbh(String qyzch) {
....
38.         return this.find("from GongShangweifa where dwzzbh =
'"+qyzch+"' order by ccsj desc");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3338:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3338
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	307	51
对象	bsid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
316.                    xml = matterService.getFormInfoXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
59.   public String getFormInfoXml(String bsid) throws Exception{
60.         String xml = this.matterDao.getFormInfoXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
802.        public String getFormInfoXml(String bsid) throws Exception{
....
806.              String sql01="from TInsFormData t where
t.bsnum='"+bsid+"' and t.formtype='0' ";
807.              List<TInsFormData> insformlist=this.find(sql01);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3339:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3339
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	348	51
对象	bsid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbForm(String sxid,String formid,String formver,String groupid,String bsid, HttpServletRequest request,

```
....
348.        public String wssbForm(String sxid,String formid,String
formver,String groupid,String bsid, HttpServletRequest request,
....
357.                    xml = matterService.getFormInfoXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
59.   public String getFormInfoXml(String bsid) throws Exception{
60.         String xml = this.matterDao.getFormInfoXml(bsid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
802.        public String getFormInfoXml(String bsid) throws Exception{
....
806.              String sql01="from TInsFormData t where
t.bsnum='"+bsid+"' and t.formtype='0' ";
807.              List<TInsFormData> insformlist=this.find(sql01);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3340:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3340
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	328	51
对象	bsid	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
336.                    xml = matterService.getFormInfoHtmlXml(bsid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
50.   public String getFormInfoHtmlXml(String bsid) throws Exception{
51.         String xml = this.matterDao.getFormInfoHtmlXml(bsid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
342.        public String getFormInfoHtmlXml(String bsid) throws
Exception{
....
345.                String sql01="from TInsFormData t where
t.bsnum='"+bsid+"' and t.formtype='0' ";
346.                List<TInsFormData> insformlist=this.find(sql01);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3341:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3341
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	348	51

对象	formid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbForm(String sxid,String formid,String formver,String groupid,String bsid, HttpServletRequest request,

```
....
348.        public String wssbForm(String sxid,String formid,String
formver,String groupid,String bsid, HttpServletRequest request,
....
354.                    xml =
matterService.getFormInfoHtmlData(sxid,formid,formver,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
54.   public String getFormInfoHtmlData(String sxid,String formid,String
formver,String groupid) {
55.         String xml =
this.matterDao.getFormInfoHtmlData(sxid,formid,formver,groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
440.        public String getFormInfoHtmlData(String sxid,String
formid,String formver,String groupid) {
....
443.              String sql02="from TXmlClob t where
t.formId='"+formid+"' and t.active='1'";
....
445.              List list = this.find(sql02);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3342:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3342
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	328	51
对象	request	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
32.   public static CmsUser getUser(HttpServletRequest request) {
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3343:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3343
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	933	51
对象	sxid	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
933.        public String getPostInfo(String sxid, HttpServletRequest
request,
....
953.                out.print(matterService.getPostInfo(sxid,user));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getPostInfo(String sxid, CmsUser user) throws Exception{

```
....
92.   public String getPostInfo(String sxid, CmsUser user) throws
Exception{
93.         List infoList = this.matterDao.findBySql("from
TWebhallPermissionitemPost t where t.sxid='"+sxid+"' and
t.changetype<>'D' ");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法	public List findBySql(String querySql) throws Exception {

```
....
947.        public List findBySql(String querySql) throws Exception {
948.              return this.find(querySql);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3344:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3344
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	960	51
对象	bsnum	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String getPostinsInfo(String bsnum, HttpServletRequest request,

```
....
960.        public String getPostinsInfo(String bsnum,
HttpServletRequest request,
....
968.              out.print(matterService.getPostInsInfo(bsnum));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getPostInsInfo(String bsnum) throws Exception{

```
....
138.        public String getPostInsInfo(String bsnum) throws Exception{
139.              List infoList = this.matterDao.findBySql("from
TWebhallPost t where t.id='"+bsnum+"' and t.changetype<>'D' ");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public List findBySql(String querySql) throws Exception {

```
....
947.        public List findBySql(String querySql) throws Exception {
948.              return this.find(querySql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3345:

严重程度： 高风险

结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3345
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	975	51
对象	bsnum	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String deletecgj(String bsnum, String permname, String starttime, String endtime, String deptname,

```
....
975.        public String deletecgj(String bsnum, String permname,
String starttime, String endtime, String deptname,
....
977.              wssbService.delMyDraft(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public boolean delMyDraft(String bsnum) {

```
....
746.        public boolean delMyDraft(String bsnum) {
747.              return wssbDao.delMyDraft(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public boolean delMyDraft(String bsnum) {

```
....
58.      public boolean delMyDraft(String bsnum) {
....
62.              String hql2 = "from TTyspGrsbclxx t where t.ywid = '" +
bsnum+ "'";
....
66.              List<TTyspGrsbclxx> grclxxlist=this.find(hql2);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

SQL Injection\路径 3346:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3346
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	176	51
对象	type	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
188.                List<TSharePermissionitem> list =
this.registrationBureauMng.getSharePermissionitemListByType(type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/RegistrationBureauMngImpl.java

方法 public List<TSharePermissionitem> getSharePermissionitemListByType(String type){

```
....
26.   public List<TSharePermissionitem>
getSharePermissionitemListByType(String type){
27.         return this.dao.getSharePermissionitemListByType(type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/RegistrationBureauDaoImpl.java

方法 public List<TSharePermissionitem> getSharePermissionitemListByType(String type){

```
....
23.   public List<TSharePermissionitem>
getSharePermissionitemListByType(String type){
24.         return this.find("select s from TSharePermissionitem
s,TWebhallPermissionitem w where s.id = w.pid and w.status = '1' and
w.ptype='"+type+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

SQL Injection\路径 3347:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3347

结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	176	101
对象	type	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/RegistrationBureauAct.java

方法 public String qiyedengji(String type ,Integer pageNo,HttpServletRequest request, ModelMap model) {

```
....
176.        public String qiyedengji(String type ,Integer
pageNo,HttpServletRequest request, ModelMap model) {
....
188.              List<TSharePermissionitem> list =
this.registrationBureauMng.getSharePermissionitemListByType(type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/RegistrationBureauMngImpl.java

方法 public List<TSharePermissionitem> getSharePermissionitemListByType(String type){

```
....
26.   public List<TSharePermissionitem>
getSharePermissionitemListByType(String type){
27.         return this.dao.getSharePermissionitemListByType(type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/RegistrationBureauDaoImpl.java

方法 public List<TSharePermissionitem> getSharePermissionitemListByType(String type){

```
....
23.   public List<TSharePermissionitem>
getSharePermissionitemListByType(String type){
24.         return this.find("select s from TSharePermissionitem
s,TWebhallPermissionitem w where s.id = w.pid and w.status = '1' and
w.ptype='"+type+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public String getOrigHql() {

```
....
46.         return hqlBuilder.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query setParamsToQuery(Query query) {

```
....
208.        public Query setParamsToQuery(Query query) {
....
242.              return query;
```

SQL Injection\路径 3348:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3348
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	215	146

对象	""enterprice""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
215.              String enterprice =
request.getParameter("enterprice");
....
218.              gasinfo.setF29e000027aa003002(enterprice);
....
231.              Pagination pagination =
enterpriseGuanZhuLanService.getPageForGasInfo(gasinfo,user.getId().toStr
ing(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public void setF29e000027aa003002(String f29e000027aa003002) {

```
....
77.   public void setF29e000027aa003002(String f29e000027aa003002) {
78.         this.f29e000027aa003002 = f29e000027aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
42.   public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
43.         return
enterpriseGuanZhuLanDao.getPageForGasInfo(gasinfo,userid,pageNo,pageSize
);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
110.        public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
....
128.              if (gasinfo.getF29e000027aa003002() != null &&
!gasinfo.getF29e000027aa003002().equals("")) {
....
130.                    sbcount.append(gasinfo.getF29e000027aa003002());
131.                    sbcount.append("%'");
....
143.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
144.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
145.              querycount.setCacheable(false);
146.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public String getF29e000027aa003002() {

```
....
73.         return f29e000027aa003002;
```

SQL Injection\路径 3349:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3349
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	317	295
对象	""enterprice""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
317.              String enterprice =
request.getParameter("enterprice");
....
320.              nationaltax.setF29e000063aa003002(enterprice);
....
333.              Pagination pagination =
enterpriseGuanZhuLanService.getPageForNationalTaxInfo(nationaltax,user.g
etId().toString(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.              this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
54.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
55.         return
enterpriseGuanZhuLanDao.getPageForNationalTaxInfo(nationaltax,userid,pag
eNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
257.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
277.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
279.
      sbcount.append(nationaltax.getF29e000063aa003002());
280.                    sbcount.append("%'");
....
292.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
293.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
294.              querycount.setCacheable(false);
295.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 3350:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3350
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	393	295
对象	""ntenterprice""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanAct.java
方法	public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
393.              String ntenterprice =
request.getParameter("ntenterprice");
....
396.              nationaltax.setF29e000063aa003002(ntenterprice);
....
409.              Pagination paginationNT =
enterpriseGuanZhuLanService.getPageForNationalTaxInfo(nationaltax,user.g
etId().toString(),cpn(pageNoNT),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.              this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
54.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
55.         return
enterpriseGuanZhuLanDao.getPageForNationalTaxInfo(nationaltax,userid,pag
eNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
257.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
277.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
279.
      sbcount.append(nationaltax.getF29e000063aa003002());
280.                    sbcount.append("%'");
....
292.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
293.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
294.              querycount.setCacheable(false);
295.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java
方法	public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 3351:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3351
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	215	145
对象	""enterprice""	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java
方法	public String guanzhulanGas(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
215.              String enterprice =
request.getParameter("enterprice");
....
218.              gasinfo.setF29e000027aa003002(enterprice);
....
231.              Pagination pagination =
enterpriseGuanZhuLanServicegr.getPageForGasInfo(gasinfo,user.getId().toS
tring(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public void setF29e000027aa003002(String f29e000027aa003002) {

```
....
77.   public void setF29e000027aa003002(String f29e000027aa003002) {
78.         this.f29e000027aa003002 = f29e000027aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
52.   public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
53.         return
enterpriseGuanZhuLanDaogr.getPageForGasInfo(gasinfo,userid,pageNo,pageSi
ze);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
109.        public Pagination getPageForGasInfo(T29e000027aa003 gasinfo
,String userid,int pageNo,int pageSize){
....
127.              if (gasinfo.getF29e000027aa003002() != null &&
!gasinfo.getF29e000027aa003002().equals("")) {
....
129.                    sbcount.append(gasinfo.getF29e000027aa003002());
130.                    sbcount.append("%'");
....
142.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
143.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
144.              querycount.setCacheable(false);
145.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000027aa003.java

方法 public String getF29e000027aa003002() {

```
....
73.         return f29e000027aa003002;
```

SQL Injection\路径 3352:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3352
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	317	294
对象	""enterprice""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanNationalTax(HttpServletRequest request,HttpServletResponse response, Integer pageNo, ModelMap model) {

```
....
317.                String enterprice =
request.getParameter("enterprice");
....
320.                nationaltax.setF29e000063aa003002(enterprice);
....
333.                Pagination pagination =
enterpriseGuanZhuLanServicegr.getPageForNationalTaxInfo(nationaltax,user
.getId().toString(),cpn(pageNo),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.                this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
64.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
65.         return
enterpriseGuanZhuLanDaogr.getPageForNationalTaxInfo(nationaltax,userid,p
ageNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
256.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
276.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
278.
      sbcount.append(nationaltax.getF29e000063aa003002());
279.                    sbcount.append("%'");
....
291.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
292.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
293.              querycount.setCacheable(false);
294.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 3353:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3353
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	393	294
对象	""ntenterprice""	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseGuanZhuLanActgr.java

方法 public String guanzhulanTaxinfo(HttpServletRequest request,HttpServletResponse response,String selectTagNo, Integer pageNo,Integer pageNoNT, ModelMap model) {

```
....
393.              String ntenterprice =
request.getParameter("ntenterprice");
....
396.              nationaltax.setF29e000063aa003002(ntenterprice);
....
409.              Pagination paginationNT =
enterpriseGuanZhuLanServicegr.getPageForNationalTaxInfo(nationaltax,user
.getId().toString(),cpn(pageNoNT),10);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public void setF29e000063aa003002(String f29e000063aa003002) {

```
....
113.        public void setF29e000063aa003002(String f29e000063aa003002)
{
114.              this.f29e000063aa003002 = f29e000063aa003002;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseGuanZhuLanServiceImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
64.   public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
65.         return
enterpriseGuanZhuLanDaogr.getPageForNationalTaxInfo(nationaltax,userid,p
ageNo,pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java

方法 public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
256.        public Pagination getPageForNationalTaxInfo(T29e000063aa003
nationaltax ,String userid,int pageNo,int pageSize){
....
276.              if (nationaltax.getF29e000063aa003002() != null &&
!nationaltax.getF29e000063aa003002().equals("")) {
....
278.
      sbcount.append(nationaltax.getF29e000063aa003002());
279.                    sbcount.append("%'");
....
291.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
292.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
293.              querycount.setCacheable(false);
294.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/T29e000063aa003.java

方法 public String getF29e000063aa003002() {

```
....
62.         return this.f29e000063aa003002;
```

SQL Injection\路径 3354:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3354
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java
行	481	147
对象	type	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getSbpzXml(String bsnum,String type, HttpServletRequest request,

```
....
481.        public String getSbpzXml(String bsnum,String type,
HttpServletRequest request,
....
490.              sqpz_xml=wssbService.getYwpzXml(bsnum,type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getYwpzXml(String bsnum,String type){

```
....
80.   public String getYwpzXml(String bsnum,String type){
....
83.                ywpz=TInsYwpzService.getYwpz(bsnum, type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.         return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3355:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3355
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzS

		erviceImpl.java
行	481	18
对象	type	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getSbpzXml(String bsnum,String type, HttpServletRequest request,

```
....
481.        public String getSbpzXml(String bsnum,String type,
HttpServletRequest request,
....
490.              sqpz_xml=wssbService.getYwpzXml(bsnum,type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getYwpzXml(String bsnum,String type){

```
....
80.   public String getYwpzXml(String bsnum,String type){
....
83.                ywpz=TInsYwpzService.getYwpz(bsnum, type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.         return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3356:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathi

	d=3356
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java
行	481	147
对象	bsnum	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getSbpzXml(String bsnum,String type, HttpServletRequest request,

```
....
481.        public String getSbpzXml(String bsnum,String type,
HttpServletRequest request,
....
490.             sqpz_xml=wssbService.getYwpzXml(bsnum,type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getYwpzXml(String bsnum,String type){

```
....
80.   public String getYwpzXml(String bsnum,String type){
....
83.               ywpz=TInsYwpzService.getYwpz(bsnum, type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.         return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3357:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3357
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java
行	481	18
对象	bsnum	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getSbpzXml(String bsnum,String type, HttpServletRequest request,

```
....
481.        public String getSbpzXml(String bsnum,String type,
HttpServletRequest request,
....
490.              sqpz_xml=wssbService.getYwpzXml(bsnum,type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getYwpzXml(String bsnum,String type){

```
....
80.   public String getYwpzXml(String bsnum,String type){
....
83.               ywpz=TInsYwpzService.getYwpz(bsnum, type);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.          return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3358:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3358
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java
行	49	147
对象	""bsnum""	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法 public void doGet(HttpServletRequest request, HttpServletResponse response)

```
....
49.              bsnum = request.getParameter("bsnum");
....
59.                    TransformerFactory tf =
TransformerFactory.newInstance();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法

```
....
102.
....
108.              }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法 StringBuffer dataSb = new StringBuffer();

```
....
127.              StringBuffer dataSb = new StringBuffer();
....
129.              String dataxml=ywpz.getDataXml();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.          return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3359:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3359
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

行	49	18
对象	""bsnum""	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法 public void doGet(HttpServletRequest request, HttpServletResponse response)

```
....
49.                bsnum = request.getParameter("bsnum");
....
59.                      TransformerFactory tf =
TransformerFactory.newInstance();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法

```
....
102.
....
108.               }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/print/servlet/ViewXmlServlet.java

方法 StringBuffer dataSb = new StringBuffer();

```
....
127.               StringBuffer dataSb = new StringBuffer();
....
129.               String dataxml=ywpz.getDataXml();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java

方法 public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
17.      public TInsYwpz getYwpz(String ywbh, String type) throws
Exception {
18.          return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3360:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3360
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java
行	498	147
对象	sxid	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
498.        public String getYzsd(String sxid,String bsnum,
HttpServletRequest request,
....
501.              sfzc_xml=wssbService.getSharePost(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getSharePost(String sxid){

```
....
96.   public String getSharePost(String sxid){
97.         TSharePost t=tsharePostService.getTSharePost(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java

方法 public TSharePost getTSharePost(String sxid) {

```
....
13.   public TSharePost getTSharePost(String sxid) {
....
15.         List list=super.find("from TSharePost t where
t.sxid='"+sxid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

SQL Injection\路径 3361:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3361
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java
行	498	15
对象	sxid	find

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
498.        public String getYzsd(String sxid,String bsnum,
HttpServletRequest request,
....
501.              sfzc_xml=wssbService.getSharePost(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getSharePost(String sxid){

```
....
96.   public String getSharePost(String sxid){
97.         TSharePost t=tsharePostService.getTSharePost(sxid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java

方法 public TSharePost getTSharePost(String sxid) {

```
....
13.   public TSharePost getTSharePost(String sxid) {
....
15.         List list=super.find("from TSharePost t where
t.sxid='"+sxid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/BaseDaoImpl.java

方法 public List find(final String query) {

```
....
145.      public List find(final String query) {
....
147.        return getHibernateTemplate().find(query);
```

Second Order SQL Injection

描述

Second Order SQL Injection\路径 963:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=963
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java
行	25	37
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getList(Integer count, boolean cacheable) {

```
....
25.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListForTag(Integer count) {

```
....
15.         return dao.getList(count, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
110.                    List<SysRegion> list =
sysRegionMng.getListForTag(100);
111.                    Iterator<SysRegion> iList = list.iterator();
112.                    while (iList.hasNext()) {
113.                          SysRegion sR = (SysRegion) iList.next();
114.                          if(sR.getParentid() == null ||
sR.getParentid().equals("")){
115.                                areaId = sR.getAreaid();
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getAreaid() {

```
....
27.         return areaid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/HdjlAct.java

方法 public String toAddZx(String sxid,HttpServletRequest request,

```
....
111.                    Object areaId =
request.getSession().getAttribute("areaId");
....
113.                    List<TSysDept> deptList = areaId ==
null?sysDeptMng.getListForTag(null):sysDeptMng.getListForTag(null,areaId
.toString().trim());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public List<TSysDept> getListForTag(Integer count,String areaId) {

```
....
17.   public List<TSysDept> getListForTag(Integer count,String areaId) {
18.         return dao.getList(count,areaId, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public List<TSysDept> getList(Integer count,String areaId, boolean cacheable) {

```
....
26.   public List<TSysDept> getList(Integer count,String areaId, boolean
cacheable) {
....
28.         if(areaId!=null && !areaId.equals("")){
29.               hql += " and t.areaId='"+areaId+"' ";
....
32.         Query query = getSession().createQuery(hql);
....
36.         query.setCacheable(cacheable);
37.         return query.list();
```

Second Order SQL Injection\路径 964:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=964
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	25	241
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getList(Integer count, boolean cacheable) {

```
....
25.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListForTag(Integer count) {

```
....
15.         return dao.getList(count, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
110.                    List<SysRegion> list =
sysRegionMng.getListForTag(100);
111.                    Iterator<SysRegion> iList = list.iterator();
112.                    while (iList.hasNext()) {
113.                          SysRegion sR = (SysRegion) iList.next();
114.                          if(sR.getParentid() == null ||
sR.getParentid().equals("")){
115.                                areaId = sR.getAreaid();
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getAreaid() {

```
....
27.         return areaid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
227.                countSql.append(areaId);
228.                countSql.append("'");
....
239.                Query querycount =
getSession().createSQLQuery(countSql.toString());
240.                querycount.setCacheable(false);
241.                List listcount = querycount.list();
```

Second Order SQL Injection\路径 965:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=965
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	25	272
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getList(Integer count, boolean cacheable) {

```
....
25.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListForTag(Integer count) {

```
....
15.         return dao.getList(count, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
110.                    List<SysRegion> list =
sysRegionMng.getListForTag(100);
111.                    Iterator<SysRegion> iList = list.iterator();
112.                    while (iList.hasNext()) {
113.                          SysRegion sR = (SysRegion) iList.next();
114.                          if(sR.getParentid() == null ||
sR.getParentid().equals("")){
115.                                areaId = sR.getAreaid();
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getAreaid() {

```
....
27.         return areaid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
562.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 966:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=966
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	25	218
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getList(Integer count, boolean cacheable) {

```
....
25.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListForTag(Integer count) {

```
....
15.         return dao.getList(count, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
110.                    List<SysRegion> list =
sysRegionMng.getListForTag(100);
111.                    Iterator<SysRegion> iList = list.iterator();
112.                    while (iList.hasNext()) {
113.                          SysRegion sR = (SysRegion) iList.next();
114.                          if(sR.getParentid() == null ||
sR.getParentid().equals("")){
115.                                areaId = sR.getAreaid();
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getAreaid() {

```
....
27.         return areaid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

Second Order SQL Injection\路径 967:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=967
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	25	247
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getList(Integer count, boolean cacheable) {

```
....
25.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListForTag(Integer count) {

```
....
15.         return dao.getList(count, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/LawGuideAct.java

方法 public String chickAreaId(String areaId,HttpServletRequest request){

```
....
110.                    List<SysRegion> list =
sysRegionMng.getListForTag(100);
111.                    Iterator<SysRegion> iList = list.iterator();
112.                    while (iList.hasNext()) {
113.                          SysRegion sR = (SysRegion) iList.next();
114.                          if(sR.getParentid() == null ||
sR.getParentid().equals("")){
115.                                areaId = sR.getAreaid();
....
119.                    request.getSession().setAttribute("areaId",
areaId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getAreaid() {

```
....
27.         return areaid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
600.              String areaid =
(String)request.getSession().getAttribute("areaId");
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
232.                sb.append(areaId);
233.                sb.append("'");
....
242.                sb.append(") tv)R WHERE R.RNUM>");
243.                sb.append((pageNo-1)*pageSize);
244.                sb.append(" AND R.RNUM<=");
245.                sb.append(pageNo*pageSize);
....
247.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 968:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=968
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	57	93
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public TSysDept getById(String id) {

```
....
65.         return super.get(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public TSysDept getById(String id) {

```
....
33.         return dao.getById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
381.              TSysDept tSysDept = sysDeptMng.getById(deptId);
....
383.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(tSysDept.getDeptId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java

方法 public String getDeptId() {

```
....
145.              return deptId;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

Second Order SQL Injection\路径 969:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=969
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	57	241
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.               entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.              CmsUser entity = get(id);
123.              return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.          CmsUser entity = dao.findById(id);
67.          return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                      user = cmsUserMng.findById(userId);
....
72.          CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.          request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.          return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
221.              countSql.append(username);
222.              countSql.append("') F ");
223.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
224.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
225.              countSql.append(name);
226.              countSql.append("%' AND T.AREAID='");
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 970:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=970
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	57	218
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
198.                countSql.append(username);
199.                countSql.append("') F ");
200.                countSql.append(" ON T.SXID = F.SERVICE_CODE");
201.                countSql.append("  WHERE T.SXZXNAME LIKE '%");
202.                countSql.append(name);
203.                countSql.append("%' AND T.AREAID='");
204.                countSql.append(areaId);
205.                countSql.append("'");
....
216.                Query querycount =
getSession().createSQLQuery(countSql.toString());
217.                querycount.setCacheable(false);
218.                List listcount = querycount.list();
```

Second Order SQL Injection\路径 971:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=971
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	57	51
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

Second Order SQL Injection\路径 972:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=972
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	57	101
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
321.                    List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public String getOrigHql() {

```
....
46.          return hqlBuilder.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query setParamsToQuery(Query query) {

```
....
208.         public Query setParamsToQuery(Query query) {
....
242.              return query;
```

Second Order SQL Injection\路径 973:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=973
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	57	272
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
250.                sb.append(username);
251.                sb.append("') F ");
252.                sb.append(" ON T.SXID = F.SERVICE_CODE");
253.                sb.append("  WHERE T.SXZXNAME LIKE '%");
254.                sb.append(name);
255.                sb.append("%' AND T.AREAID='");
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 974:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=974
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	57	247
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
226.              sb.append(username);
227.              sb.append("') F ");
228.              sb.append(" ON T.SXID = F.SERVICE_CODE");
229.              sb.append("  WHERE T.SXZXNAME LIKE '%");
230.              sb.append(name);
231.              sb.append("%' AND T.AREAID='");
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 975:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-

	9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=975
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	57	108
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findById(Integer id) {

```
....
36.         CmsSite entity = get(id);
37.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findById(Integer id) {

```
....
45.         CmsSite entity = dao.findById(id);
46.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
195.                            if (site != null) {
....
200.                            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
172.                if (site == null) {
....
185.                }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.          CmsSite site = getSite(request, response);
50.          CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.    public static void setSite(HttpServletRequest request, CmsSite
site) {
78.          request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.          return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法	public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java
方法	public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
方法	public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 976:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=976
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	60	93
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public TSysDept getById(String id) {

```
....
65.         return super.get(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public TSysDept getById(String id) {

```
....
33.         return dao.getById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
381.                TSysDept tSysDept = sysDeptMng.getById(deptId);
....
383.                List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(tSysDept.getDeptId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java

方法 public String getDeptId() {

```
....
145.                return deptId;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

Second Order SQL Injection\路径 977:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=977
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	60	241
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.               entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
221.              countSql.append(username);
222.              countSql.append("') F ");
223.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
224.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
225.              countSql.append(name);
226.              countSql.append("%' AND T.AREAID='");
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 978:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=978
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	60	218
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
198.              countSql.append(username);
199.              countSql.append("') F ");
200.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
201.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
202.              countSql.append(name);
203.              countSql.append("%' AND T.AREAID='");
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 979:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=979
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	60	51
对象	get	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java
方法	protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

Second Order SQL Injection\路径 980:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=980
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	60	101
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
321.                    List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public String getOrigHql() {

```
....
46.         return hqlBuilder.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query setParamsToQuery(Query query) {

```
....
208.        public Query setParamsToQuery(Query query) {
....
242.              return query;
```

Second Order SQL Injection\路径 981:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=981

结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	60	272
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
250.              sb.append(username);
251.              sb.append("') F ");
252.              sb.append(" ON T.SXID = F.SERVICE_CODE");
253.              sb.append("  WHERE T.SXZXNAME LIKE '%");
254.              sb.append(name);
255.              sb.append("%' AND T.AREAID='");
256.              sb.append(areaId);
257.              sb.append("'");
....
267.              sb.append(") tv)R WHERE R.RNUM>");
268.              sb.append((pageNo-1)*pageSize);
269.              sb.append(" AND R.RNUM<=");
270.              sb.append(pageNo*pageSize);
....
272.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 982:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=982
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	60	247
对象	get	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java
方法	protected T get(ID id, boolean lock) {

```
....
60.               entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
226.              sb.append(username);
227.              sb.append("') F ");
228.              sb.append(" ON T.SXID = F.SERVICE_CODE");
229.              sb.append("  WHERE T.SXZXNAME LIKE '%");
230.              sb.append(name);
231.              sb.append("%' AND T.AREAID='");
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 983:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=983
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	60	108
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.                 entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findById(Integer id) {

```
....
36.         CmsSite entity = get(id);
37.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findById(Integer id) {

```
....
45.         CmsSite entity = dao.findById(id);
46.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
195.                            if (site != null) {
....
200.                            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
172.                if (site == null) {
....
185.                }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java
方法	public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java
方法	public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
方法	public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 984:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=984
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	51	93

对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public TSysDept getById(String id) {

```
....
65.         return super.get(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public TSysDept getById(String id) {

```
....
33.         return dao.getById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
381.             TSysDept tSysDept = sysDeptMng.getById(deptId);
....
383.             List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(tSysDept.getDeptId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java

方法 public String getDeptId() {

```
....
145.              return deptId;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

Second Order SQL Injection\路径 985:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=985
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	241
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.              CmsUser entity = get(id);
123.              return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
221.              countSql.append(username);
222.              countSql.append("') F ");
223.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
224.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
225.              countSql.append(name);
226.              countSql.append("%' AND T.AREAID='");
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 986:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=986
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	218
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
方法	public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
198.              countSql.append(username);
199.              countSql.append("') F ");
200.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
201.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
202.              countSql.append(name);
203.              countSql.append("%' AND T.AREAID='");
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 987:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=987
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	51	51
对象	get	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java
方法	public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.                Query queryObject =
getSession().createQuery(queryString);
....
116.                return queryObject;
```

Second Order SQL Injection\路径 988:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=988
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	51	101
对象	get	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java
方法	public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.          return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                     CmsUser user = CmsUtils.getUser(request);
333.                     xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.          String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.         public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.         public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
321.                   List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法	protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java
方法	public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java
方法	public String getOrigHql() {

```
....
46.         return hqlBuilder.toString();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java
方法	public Query setParamsToQuery(Query query) {

```
....
208.        public Query setParamsToQuery(Query query) {
....
242.              return query;
```

Second Order SQL Injection\路径 989:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=989
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	51	272

对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
250.                sb.append(username);
251.                sb.append("') F ");
252.                sb.append(" ON T.SXID = F.SERVICE_CODE");
253.                sb.append("  WHERE T.SXZXNAME LIKE '%");
254.                sb.append(name);
255.                sb.append("%' AND T.AREAID='");
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 990:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=990
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	51	247
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
226.              sb.append(username);
227.              sb.append("') F ");
228.              sb.append(" ON T.SXID = F.SERVICE_CODE");
229.              sb.append("  WHERE T.SXZXNAME LIKE '%");
230.              sb.append(name);
231.              sb.append("%' AND T.AREAID='");
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 991:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-

	9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=991
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	51	108
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SyncConfigDaoImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
51.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findById(Integer id) {

```
....
36.         CmsSite entity = get(id);
37.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findById(Integer id) {

```
....
45.         CmsSite entity = dao.findById(id);
46.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
195.                            if (site != null) {
....
200.                            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
172.                if (site == null) {
....
185.                }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法 public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java

方法 public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java

方法 public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 992:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=992
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	43	93
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public TSysDept getById(String id) {

```
....
65.         return super.get(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public TSysDept getById(String id) {

```
....
33.         return dao.getById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
381.              TSysDept tSysDept = sysDeptMng.getById(deptId);
....
383.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(tSysDept.getDeptId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java

方法 public String getDeptId() {

```
....
145.              return deptId;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

Second Order SQL Injection\路径 993:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=993
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	43	241
对象	get	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java
方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java
方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
221.              countSql.append(username);
222.              countSql.append("') F ");
223.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
224.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
225.              countSql.append(name);
226.              countSql.append("%' AND T.AREAID='");
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 994:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=994

结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	43	218
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.           return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.                CmsUser entity = get(id);
123.                return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.           CmsUser entity = dao.findById(id);
67.           return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
198.              countSql.append(username);
199.              countSql.append("') F ");
200.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
201.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
202.              countSql.append(name);
203.              countSql.append("%' AND T.AREAID='");
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 995:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=995
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	43	51
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

Second Order SQL Injection\路径 996:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=996
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	43	101
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
321.                    List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public String getOrigHql() {

```
....
46.          return hqlBuilder.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query setParamsToQuery(Query query) {

```
....
208.         public Query setParamsToQuery(Query query) {
....
242.              return query;
```

Second Order SQL Injection\路径 997:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=997
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	43	272
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.              CmsUser entity = get(id);
123.              return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
250.                sb.append(username);
251.                sb.append("') F ");
252.                sb.append(" ON T.SXID = F.SERVICE_CODE");
253.                sb.append("  WHERE T.SXZXNAME LIKE '%");
254.                sb.append(name);
255.                sb.append("%' AND T.AREAID='");
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 998:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=998
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	43	247
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.        return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
226.              sb.append(username);
227.              sb.append("') F ");
228.              sb.append(" ON T.SXID = F.SERVICE_CODE");
229.              sb.append("  WHERE T.SXZXNAME LIKE '%");
230.              sb.append(name);
231.              sb.append("%' AND T.AREAID='");
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 999:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-

	9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=999
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	43	108
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findById(Integer id) {

```
....
36.         CmsSite entity = get(id);
37.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findById(Integer id) {

```
....
45.         CmsSite entity = dao.findById(id);
46.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
195.                            if (site != null) {
....
200.                            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
172.                if (site == null) {
....
185.                }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法 public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java

方法 public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java

方法 public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 1000:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1000
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java
行	55	93
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysDeptDaoImpl.java

方法 public TSysDept getById(String id) {

```
....
65.         return super.get(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysDeptMngImpl.java

方法 public TSysDept getById(String id) {

```
....
33.         return dao.getById(id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/ZwgkAct.java

方法 public String lawproduce(HttpServletRequest request,

```
....
381.              TSysDept tSysDept = sysDeptMng.getById(deptId);
....
383.              List<TSysDeptWindow> deptWindowList =
deptWindowMng.getDeptWindowsByDeptId(tSysDept.getDeptId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysDept.java

方法 public String getDeptId() {

```
....
145.              return deptId;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/DeptWindowMngImpl.java

方法 public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId) {

```
....
27.   public List<TSysDeptWindow> getDeptWindowsByDeptId(String deptId)
{
28.         return dao.getWindowInfoByDeptId(deptId);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/DeptWindowDaoImpl.java

方法 public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {

```
....
86.   public List<TSysDeptWindow> getWindowInfoByDeptId(String deptId) {
....
90.         String hql = "from TSysDeptWindow t where t.changetype <>
'D' and t.deptid = '"+deptId+"' order by t.name";
91.         Query query = getSession().createQuery(hql);
92.         query.setCacheable(true);
93.         return query.list();
```

Second Order SQL Injection\路径 1001:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1001
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	241
对象	get	list

代码片断
文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java
方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java
方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
221.              countSql.append(username);
222.              countSql.append("') F ");
223.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
224.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
225.              countSql.append(name);
226.              countSql.append("%' AND T.AREAID='");
227.              countSql.append(areaId);
228.              countSql.append("'");
....
239.              Query querycount =
getSession().createSQLQuery(countSql.toString());
240.              querycount.setCacheable(false);
241.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 1002:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1002

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	218
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
198.              countSql.append(username);
199.              countSql.append("') F ");
200.              countSql.append(" ON T.SXID = F.SERVICE_CODE");
201.              countSql.append("  WHERE T.SXZXNAME LIKE '%");
202.              countSql.append(name);
203.              countSql.append("%' AND T.AREAID='");
204.              countSql.append(areaId);
205.              countSql.append("'");
....
216.              Query querycount =
getSession().createSQLQuery(countSql.toString());
217.              querycount.setCacheable(false);
218.              List listcount = querycount.list();
```

Second Order SQL Injection\路径 1003:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1003
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	55	51
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
320.                    List<TWebHallIncInforMation> webhallinclist =
this.find("from TWebHallIncInforMation where incid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

Second Order SQL Injection\路径 1004:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1004
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	55	101
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
332.                    CmsUser user = CmsUtils.getUser(request);
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
135.              String userJson = getFormHtmlXml(userid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
315.        public String getFormHtmlXml(String userid){
....
318.              if(userid!=null&&!userid.equals("")){
....
321.                    List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
99.   protected List find(Finder finder) {
100.              Query query = finder.createQuery(getSession());
101.              List list = query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query createQuery(Session s) {

```
....
246.              Query query =
setParamsToQuery(s.createQuery(getOrigHql()));
....
256.              return query;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public String getOrigHql() {

```
....
46.         return hqlBuilder.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public Query setParamsToQuery(Query query) {

```
....
208.        public Query setParamsToQuery(Query query) {
....
242.              return query;
```

Second Order SQL Injection\路径 1005:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1005
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java
行	55	272
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.              CmsUser entity = get(id);
123.              return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingAct.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
550.              CmsUser user = CmsUtils.getUser(request);
....
570.              Pagination p =
enterpriseBanShiTingService.getPageForSelPermissionitem(user.getUsername
(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImpl.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
60.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
62.         return enterpriseBanShiTingDao.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImpl.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
216.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
250.                sb.append(username);
251.                sb.append("') F ");
252.                sb.append(" ON T.SXID = F.SERVICE_CODE");
253.                sb.append("  WHERE T.SXZXNAME LIKE '%");
254.                sb.append(name);
255.                sb.append("%' AND T.AREAID='");
256.                sb.append(areaId);
257.                sb.append("'");
....
267.                sb.append(") tv)R WHERE R.RNUM>");
268.                sb.append((pageNo-1)*pageSize);
269.                sb.append(" AND R.RNUM<=");
270.                sb.append(pageNo*pageSize);
....
272.                List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 1006:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1006
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java
行	55	247
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsUserDaoImpl.java

方法 public CmsUser findById(Integer id) {

```
....
122.             CmsUser entity = get(id);
123.             return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsUserMngImpl.java

方法 public CmsUser findById(Integer id) {

```
....
66.         CmsUser entity = dao.findById(id);
67.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
68.                     user = cmsUserMng.findById(userId);
....
72.         CmsUtils.setUser(request, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setUser(HttpServletRequest request, CmsUser user) {

```
....
57.   public static void setUser(HttpServletRequest request, CmsUser
user) {
58.         request.setAttribute(USER_KEY, user);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsUser getUser(HttpServletRequest request) {

```
....
33.         return (CmsUser) request.getAttribute(USER_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String banshitingselpermissionitem(HttpServletRequest request,

```
....
588.              CmsUser user = CmsUtils.getUser(request);
....
608.              Pagination p =
enterpriseBanShiTingServicegr.getPageForSelPermissionitem(user.getUserna
me(),com.jeecms.cms.CTools.getStringAdd(name,"%"),areaid,orderBy,
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/EnterpriseBanShiTingServiceImplgr.java

方法 public Pagination getPageForSelPermissionitem(String username,String name,String areaId,String orderBy, Integer siteId,

```
....
62.   public Pagination getPageForSelPermissionitem(String
username,String name,String areaId,String orderBy, Integer siteId,
....
64.         return enterpriseBanShiTingDaogr.getSelPage(username,name,
areaId, orderBy, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseBanShiTingDaoImplgr.java

方法 public Pagination getSelPage(String username,String name, String areaId,String orderBy, int pageNo, int pageSize) {

```
....
194.        public Pagination getSelPage(String username,String name,
String areaId,String orderBy, int pageNo, int pageSize) {
....
226.              sb.append(username);
227.              sb.append("') F ");
228.              sb.append(" ON T.SXID = F.SERVICE_CODE");
229.              sb.append("  WHERE T.SXZXNAME LIKE '%");
230.              sb.append(name);
231.              sb.append("%' AND T.AREAID='");
232.              sb.append(areaId);
233.              sb.append("'");
....
242.              sb.append(") tv)R WHERE R.RNUM>");
243.              sb.append((pageNo-1)*pageSize);
244.              sb.append(" AND R.RNUM<=");
245.              sb.append(pageNo*pageSize);
....
247.              List<Map<String, String>> list =
getSession().createSQLQuery(sb.toString()).setResultTransformer(Transfor
mers.ALIAS_TO_ENTITY_MAP).list();
```

Second Order SQL Injection\路径 1007:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-

	9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1007
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	55	108
对象	get	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public Object get(Class clazz, Serializable id) {

```
....
55.         return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id) {

```
....
42.         return get(id, false);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findById(Integer id) {

```
....
36.         CmsSite entity = get(id);
37.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findById(Integer id) {

```
....
45.         CmsSite entity = dao.findById(id);
46.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
195.                            if (site != null) {
....
200.                            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
172.                if (site == null) {
....
185.                }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法 public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java

方法 public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java

方法 public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 1008:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1008
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
行	511	570
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
511.              for(Object
sb:this.getSession().createSQLQuery(sql.toString()).list()){
....
524.
      xml.append("<gid>"+changeStr(temp[3].toString())+"</gid>");
....
540.
      xml.append("<uid>"+changeStr(temp[6].toString())+"</uid>");
....
550.                           if(null !=
element.element("materialname").getText() &&
element.element("materialname").getText().equals(temp[1].toString())){
....
569.                                  String sql2 = "select t.sfby from
t_share_sxclgl t where t.clid = '"+temp[0].toString()+"' and
t.sxid='"+sxid+"'";
570.                                  List list =
getSession().createSQLQuery(sql2).list();
```

Second Order SQL Injection\路径 1009:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1009
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	32	108
对象	uniqueResult	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public CmsSite findByDomain(String domain, boolean cacheable) {

```
....
32.         return (CmsSite) query.uniqueResult();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public CmsSite findByDomain(String domain, boolean cacheable) {

```
....
40.         return dao.findByDomain(domain, cacheable);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 String domain = request.getServerName();

```
....
228.            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
177.            }
....
185.            }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java
方法	public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java
方法	public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
方法	public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 1010:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1010
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java
行	25	108

对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSiteDaoImpl.java

方法 public List<CmsSite> getList(boolean cacheable) {

```
....
25.         return
getSession().createQuery(hql).setCacheable(cacheable).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsSiteMngImpl.java

方法 public List<CmsSite> getListFromCache() {

```
....
35.         return dao.getList(true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 List<CmsSite> list = cmsSiteMng.getListFromCache();

```
....
234.             if (list.size() > 0) {
235.                 return list.get(0);
236.             } else {
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 HttpServletResponse response) {

```
....
180.             }
....
185.             }
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/AdminContextInterceptor.java

方法 public boolean preHandle(HttpServletRequest request,

```
....
49.         CmsSite site = getSite(request, response);
50.         CmsUtils.setSite(request, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static void setSite(HttpServletRequest request, CmsSite site) {

```
....
77.   public static void setSite(HttpServletRequest request, CmsSite
site) {
78.         request.setAttribute(SITE_KEY, site);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/CmsUtils.java

方法 public static CmsSite getSite(HttpServletRequest request) {

```
....
68.         return (CmsSite) request.getAttribute(SITE_KEY);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/THrUserAct.java

方法 public String exportAll(String id, HttpServletRequest request,HttpServletResponse response,

```
....
1042.                                       CmsSite site =
CmsUtils.getSite(request);
1043.                                       List<THrUser> tHrUserList =
tHrUserService.getListForTag(String.valueOf(site.getId()));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/THrUserServiceImpl.java

方法 public List<THrUser> getListForTag(String site) {

```
....
70.   public List<THrUser> getListForTag(String site) {
71.         return dao.getList(site, true);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/THrUserDaoImpl.java

方法 public List<THrUser> getList(String site,boolean cacheable) {

```
....
101.        public List<THrUser> getList(String site,boolean cacheable)
{
....
104.                    hql += " and t.site_id = '" + site + "'";
....
106.              Query query = getSession().createQuery(hql);
107.              query.setCacheable(cacheable);
108.              return query.list();
```

Second Order SQL Injection\路径 1011:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1011
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/UnifiedUserDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinessDaoImpl.java
行	86	205
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/dao/impl/UnifiedUserDaoImpl.java

方法 public UnifiedUser findUsernameAndPwd(String username, String password) {

```
....
86.         List<UnifiedUser> list = query.list();
....
88.               return list.get(0);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser findUsernameAndPwd(String username,String password){

```
....
379.              return dao.findUsernameAndPwd(username, password);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/webservices/service/impl/HPServiceImpl.java

方法 public String queryBusiness(String username,String password) throws Exception {

```
....
216.              UnifiedUser user =
this.unifiedUserMng.findUsernameAndPwd(username, password);
....
218.                    List<VTInsWebhallBusiness> list =
this.webhallBusinessMng.getBusinessinfoByUid(user.getId()+"");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebhallBusinessMngImpl.java

方法	public List<VTInsWebhallBusiness> getBusinessinfoByUid(String userid){

```
....
56.   public List<VTInsWebhallBusiness> getBusinessinfoByUid(String
userid){
57.         return this.dao.getBusinessinfoByUid(userid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebhallBusinessDaoImpl.java
方法	public List<VTInsWebhallBusiness> getBusinessinfoByUid(String userid) {

```
....
203.        public List<VTInsWebhallBusiness>
getBusinessinfoByUid(String userid) {
204.              String hql = "select bean from VTInsWebhallBusiness
bean where  bean.applicantid='"+userid+"' order by bean.createtime
desc";
205.              return this.getSession().createQuery(hql).list();
```

Second Order SQL Injection\路径 1012:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1012
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
行	208	51
对象	list	list

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
209.              Object[] temp = (Object[]) o;
....
214.              xml.append("<xid>"+temp[3].toString()+"</xid>");
....
218.              xml.append("<formid>"+temp[3].toString()+"</formid>");
219.
      xml.append("<formver>"+temp[6].toString()+"</formver>");
....
236.              String html = getFormInfoHtmlData(sxid,
temp[3].toString(), temp[6].toString(),groupid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
440.        public String getFormInfoHtmlData(String sxid,String
formid,String formver,String groupid) {
....
443.              String sql02="from TXmlClob t where
t.formId='"+formid+"' and t.active='1'";
....
445.              List list = this.find(sql02);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
50.   protected List find(String hql, Object... values) {
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected Query createQuery(String queryString, Object... values) {

```
....
108.        protected Query createQuery(String queryString, Object...
values) {
....
110.              Query queryObject =
getSession().createQuery(queryString);
....
116.              return queryObject;
```

Second Order SQL Injection\路径 1013:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1013
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	116	146
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
116.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
122.              for(int i=0;i<list1.size();i++){
....
124.
      sbcount.append(list1.get(i).get("INC_NAME").toString());
125.                    sbcount.append("','");
....
127.              sbcount.append("')");
....
143.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
144.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
145.              querycount.setCacheable(false);
146.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1014:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1014
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java	cms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	116	182
对象	list	list

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java

方法 public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
116.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
122.              for(int i=0;i<list1.size();i++){
....
153.              for(int i=0;i<list1.size();i++){
....
155.
      sb.append(list1.get(i).get("INC_NAME").toString());
156.                    sb.append("','");
....
158.              sb.append("')");
....
174.              sb.append(" order by bean.TOPIC_ADD_TIME desc");
....
176.              sb.append(")R WHERE R.RNUM>");
177.              sb.append((pageNo-1)*pageSize);
178.              sb.append(" AND R.RNUM<=");
179.              sb.append(pageNo*pageSize);
180.              Query query =
getSession().createSQLQuery(sb.toString());
181.              query.setCacheable(false);
182.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1015:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1015

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	263	295
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
方法	public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
263.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
270.              for(int i=0;i<list1.size();i++){
....
272.
      sbcount.append(list1.get(i).get("INC_NAME").toString());
273.                    sbcount.append("','");
....
275.              sbcount.append("')");
....
292.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
293.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
294.              querycount.setCacheable(false);
295.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1016:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1016
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
行	263	332
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImpl.java
方法	public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
263.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
270.              for(int i=0;i<list1.size();i++){
....
303.              for(int i=0;i<list1.size();i++){
....
305.
      sb.append(list1.get(i).get("INC_NAME").toString());
306.                    sb.append("','");
....
308.              sb.append("')");
....
325.              sb.append(" order by bean.TOPIC_ADD_TIME desc");
326.              sb.append(")R WHERE R.RNUM>");
327.              sb.append((pageNo-1)*pageSize);
328.              sb.append(" AND R.RNUM<=");
329.              sb.append(pageNo*pageSize);
330.              Query query =
getSession().createSQLQuery(sb.toString());
331.              query.setCacheable(false);
332.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1017:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1017
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	115	145
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
方法	public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
115.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
121.              for(int i=0;i<list1.size();i++){
....
123.
      sbcount.append(list1.get(i).get("INC_NAME").toString());
124.                    sbcount.append("','");
....
126.              sbcount.append("')");
....
142.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
143.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
144.              querycount.setCacheable(false);
145.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1018:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1018
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	115	181
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
方法	public Pagination getPageForGasInfo(T29e000027aa003 gasinfo ,String userid,int pageNo,int pageSize){

```
....
115.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
121.              for(int i=0;i<list1.size();i++){
....
152.              for(int i=0;i<list1.size();i++){
....
154.
      sb.append(list1.get(i).get("INC_NAME").toString());
155.                    sb.append("',");
....
157.              sb.append("')");
....
173.              sb.append(" order by bean.TOPIC_ADD_TIME desc");
....
175.              sb.append(")R WHERE R.RNUM>");
176.              sb.append((pageNo-1)*pageSize);
177.              sb.append(" AND R.RNUM<=");
178.              sb.append(pageNo*pageSize);
179.              Query query =
getSession().createSQLQuery(sb.toString());
180.              query.setCacheable(false);
181.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1019:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1019
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	262	294
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
方法	public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
262.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
269.              for(int i=0;i<list1.size();i++){
....
271.
      sbcount.append(list1.get(i).get("INC_NAME").toString());
272.                    sbcount.append("',");
....
274.              sbcount.append("')");
....
291.              sbcount.append(" order by bean.TOPIC_ADD_TIME desc");
292.              Query querycount =
getSession().createSQLQuery(sbcount.toString());
293.              querycount.setCacheable(false);
294.              List<Map<String, String>> listcount =
querycount.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Second Order SQL Injection\路径 1020:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=1020
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
行	262	331
对象	list	list

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/EnterpriseGuanZhuLanDaoImplgr.java
方法	public Pagination getPageForNationalTaxInfo(T29e000063aa003 nationaltax ,String userid,int pageNo,int pageSize){

```
....
262.              List<Map<String, String>> list1 =
query1.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list();
....
269.              for(int i=0;i<list1.size();i++){
....
302.              for(int i=0;i<list1.size();i++){
....
304.
      sb.append(list1.get(i).get("INC_NAME").toString());
305.                    sb.append("',");
....
307.              sb.append("')");
....
324.              sb.append(" order by bean.TOPIC_ADD_TIME desc");
325.              sb.append(")R WHERE R.RNUM>");
326.              sb.append((pageNo-1)*pageSize);
327.              sb.append(" AND R.RNUM<=");
328.              sb.append(pageNo*pageSize);
329.              Query query =
getSession().createSQLQuery(sb.toString());
330.              query.setCacheable(false);
331.              List<Map<String, String>>
list=query.setResultTransformer(Transformers.ALIAS_TO_ENTITY_MAP).list()
;
```

Side Channel Data Leakage

描述

Side Channel Data Leakage\路径 25:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=25
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	67	74
对象	password	info

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String update(Integer id, String email, String password,

```
....
67.   public String update(Integer id, String email, String password,
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
335.        public UnifiedUser update(Integer id, String password,
String email) {
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

Side Channel Data Leakage\路径 26:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=26
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	73	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
335.        public UnifiedUser update(Integer id, String password,
String email) {
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

Side Channel Data Leakage\路径 27:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=27
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
行	281	160
对象	MEMBER_PASSWORD	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/MemberAct.java

方法 public String passwordInput(HttpServletRequest request,

```
....
281.                            TPLDIR_MEMBER, MEMBER_PASSWORD);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java

方法 public static String getTplPath(HttpServletRequest request,

```
....
159.                    String solution, String dir, String name) {
....
161.                            + MessageResolver.getMessage(request,
name) + TPL_SUFFIX);
....
160.                System.out.println("模板路径=====""+solution + "/" +
dir + "/"
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/MessageResolver.java

方法 public static String getMessage(HttpServletRequest request, String code,

```
....
31.   public static String getMessage(HttpServletRequest request, String
code,
....
46.         return messageSource.getMessage(code, args, locale);
```

Side Channel Data Leakage\路径 28:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=28
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	73	61
对象	password	info

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.                user.setPassword(pwdEncoder.encodePassword(password));
311.                user.setRegisterIp(ip);
312.                user.setRegisterTime(now);
313.                user.setLastLoginIp(ip);
314.                user.setLastLoginTime(now);
315.                user.setActivation(activation);
316.                user.init();
....
323.                return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.                this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.                return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 29:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=29

结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	73	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 30:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=30
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	73	70
对象	password	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AttachmentAct.java

方法 public void url(Integer cid, Integer n, HttpServletRequest request,

```
....
85.               key = pwdEncoder.encodePassword(cid + ";" + i + ";" +
t, code);
86.               arr.put("&t=" + t + "&k=" + key);
....
88.         ResponseUtils.renderText(response, arr.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderText(HttpServletResponse response, String text) {

```
....
28.   public static void renderText(HttpServletResponse response, String
text) {
29.         render(response, "text/plain;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 31:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=31
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	76	61
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
76.                 password = "";
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.              user.setPassword(pwdEncoder.encodePassword(password));
311.              user.setRegisterIp(ip);
312.              user.setRegisterTime(now);
313.              user.setLastLoginIp(ip);
314.              user.setLastLoginTime(now);
315.              user.setActivation(activation);
316.              user.init();
....
323.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 32:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=32
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	76	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
76.                 password = "";
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 33:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=33
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	76	70
对象	password	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
76.                 password = "";
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AttachmentAct.java

方法 public void url(Integer cid, Integer n, HttpServletRequest request,

```
....
85.                 key = pwdEncoder.encodePassword(cid + ";" + i + ";" +
t, code);
86.                 arr.put("&t=" + t + "&k=" + key);
....
88.         ResponseUtils.renderText(response, arr.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderText(HttpServletResponse response, String text) {

```
....
28.   public static void renderText(HttpServletResponse response, String
text) {
29.         render(response, "text/plain;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 34:

严重程度： 高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=34
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	86	61
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
86.                 return password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.              user.setPassword(pwdEncoder.encodePassword(password));
311.              user.setRegisterIp(ip);
312.              user.setRegisterTime(now);
313.              user.setLastLoginIp(ip);
314.              user.setLastLoginTime(now);
315.              user.setActivation(activation);
316.              user.init();
....
323.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 35:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=35
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	86	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
86.                 return password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.                return user;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java
方法	public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 36:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=36
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	86	70
对象	password	write

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	protected String mergePasswordAndSalt(String password, Object salt,

```
....
86.             return password;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AttachmentAct.java

方法 public void url(Integer cid, Integer n, HttpServletRequest request,

```
....
85.                 key = pwdEncoder.encodePassword(cid + ";" + i + ";" +
t, code);
86.                 arr.put("&t=" + t + "&k=" + key);
....
88.         ResponseUtils.renderText(response, arr.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderText(HttpServletResponse response, String text) {

```
....
28.   public static void renderText(HttpServletResponse response, String
text) {
29.         render(response, "text/plain;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 37:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=37
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	88	61
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.                user.setPassword(pwdEncoder.encodePassword(password));
311.                user.setRegisterIp(ip);
312.                user.setRegisterTime(now);
313.                user.setLastLoginIp(ip);
314.                user.setLastLoginTime(now);
315.                user.setActivation(activation);
316.                user.init();
....
323.                return user;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java
方法	public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java
方法	public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 38:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=38
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	88	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.                 return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.         public void setPassword (java.lang.String password) {
210.                 this.password = password;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 39:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=39
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	88	70
对象	password	write

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	protected String mergePasswordAndSalt(String password, Object salt,

```
....
88.                 return password + "{" + salt.toString() + "}";
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java
方法	public String encodePassword(String rawPass, String salt) {

```
....
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                 digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/AttachmentAct.java

方法 public void url(Integer cid, Integer n, HttpServletRequest request,

```
....
85.                 key = pwdEncoder.encodePassword(cid + ";" + i + ";" +
t, code);
86.                 arr.put("&t=" + t + "&k=" + key);
....
88.           ResponseUtils.renderText(response, arr.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderText(HttpServletResponse response, String text) {

```
....
28.    public static void renderText(HttpServletResponse response, String
text) {
29.           render(response, "text/plain;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 40:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=40
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	22	61
对象	PROP_PASSWORD	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public static String PROP_PASSWORD = "password";

```
....
22.   public static String PROP_PASSWORD = "password";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.              user.setPassword(pwdEncoder.encodePassword(password));
311.              user.setRegisterIp(ip);
312.              user.setRegisterTime(now);
313.              user.setLastLoginIp(ip);
314.              user.setLastLoginTime(now);
315.              user.setActivation(activation);
316.              user.init();
....
323.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 41:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=41
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	22	74
对象	PROP_PASSWORD	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public static String PROP_PASSWORD = "password";

```
....
22.    public static String PROP_PASSWORD = "password";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
       user.setPassword(pwdEncoder.encodePassword(password));
....
345.               return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String update(Integer id, String email, String password,

```
....
73.          UnifiedUser user = manager.update(id, password, email);
74.          log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 42:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=42
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngI	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUser

	mpl.java	Act.java
行	303	61
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
303.        public UnifiedUser save(String username, String email,
String password,
....
310.                user.setPassword(pwdEncoder.encodePassword(password));
311.                user.setRegisterIp(ip);
312.                user.setRegisterTime(now);
313.                user.setLastLoginIp(ip);
314.                user.setLastLoginTime(now);
315.                user.setActivation(activation);
316.                user.init();
....
323.                return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.                digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
86.               return password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 43:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=43
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/core/manager/impl/UnifiedUserMngImpl.java	cms/cms/action/admin/main/UnifiedUserAct.java
行	310	61
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.              user.setPassword(pwdEncoder.encodePassword(password));
311.              user.setRegisterIp(ip);
312.              user.setRegisterTime(now);
313.              user.setLastLoginIp(ip);
314.              user.setLastLoginTime(now);
315.              user.setActivation(activation);
316.              user.init();
....
323.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
86.               return password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String save(String username, String email, String password,

```
....
59.         UnifiedUser user = manager.save(username, email, password,
request
....
62.                         .getUsername());
....
61.         log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 44:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=44
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jee	/WebHallCMSV3.0BAProject/src/com/jee

	cms/core/manager/impl/UnifiedUserMngImpl.java	cms/cms/action/admin/main/UnifiedUserAct.java
行	335	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
335.        public UnifiedUser update(Integer id, String password,
String email) {
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java

方法 public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 45:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=45
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	343	74
对象	password	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass) {

```
....
16.   public String encodePassword(String rawPass) {
17.         return encodePassword(rawPass, defaultSalt);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 public String encodePassword(String rawPass, String salt) {

```
....
20.   public String encodePassword(String rawPass, String salt) {
21.         String saltedPass = mergePasswordAndSalt(rawPass, salt,
false);
....
25.               digest =
messageDigest.digest(saltedPass.getBytes("UTF-8"));
....
29.         return new String(Hex.encodeHex(digest));
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/security/encoder/Md5PwdEncoder.java

方法 protected String mergePasswordAndSalt(String password, Object salt,

```
....
73.   protected String mergePasswordAndSalt(String password, Object
salt,
....
88.               return password + "{" + salt.toString() + "}";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public void setPassword (java.lang.String password) {

```
....
209.        public void setPassword (java.lang.String password) {
210.              this.password = password;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 46:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=46
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
行	152	160
对象	PASSWORD_RESET	println

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ForgotPasswordAct.java
方法	public String passwordReset(Integer uid, String key,

```
....
152.                            TPLDIR_MEMBER, PASSWORD_RESET);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/web/FrontUtils.java
方法	public static String getTplPath(HttpServletRequest request,

```
....
159.                        String solution, String dir, String name) {
....
161.                              + MessageResolver.getMessage(request,
name) + TPL_SUFFIX);
....
160.                System.out.println("模板路径======"+solution + "/" +
dir + "/"
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/springmvc/MessageResolver.java

方法 public static String getMessage(HttpServletRequest request, String code,

```
....
31.   public static String getMessage(HttpServletRequest request, String
code,
....
46.         return messageSource.getMessage(code, args, locale);
```

Side Channel Data Leakage\路径 47:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=47
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	33	61
对象	PROP_RESET_PWD	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java

方法 public static String PROP_RESET_PWD = "resetPwd";

```
....
33.   public static String PROP_RESET_PWD = "resetPwd";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法 public UnifiedUser save(String username, String email, String password,

```
....
310.            user.setPassword(pwdEncoder.encodePassword(password));
311.            user.setRegisterIp(ip);
312.            user.setRegisterTime(now);
313.            user.setLastLoginIp(ip);
314.            user.setLastLoginTime(now);
315.            user.setActivation(activation);
316.            user.init();
....
323.            return user;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java
方法	public UnifiedUser save(String username, String email, String password,

```
....
300.              return save(username, email, password, ip, true, null,
null);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String save(String username, String email, String password,

```
....
59.          UnifiedUser user = manager.save(username, email, password,
request
....
62.                          .getUsername());
....
61.          log.info("save UnifiedUser id={}, username={}",
user.getId(), user
```

Side Channel Data Leakage\路径 48:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=48
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
行	33	74
对象	PROP_RESET_PWD	info

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/entity/base/BaseUnifiedUser.java
方法	public static String PROP_RESET_PWD = "resetPwd";

```
....
33.   public static String PROP_RESET_PWD = "resetPwd";
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/core/manager/impl/UnifiedUserMngImpl.java

方法	public UnifiedUser update(Integer id, String password, String email) {

```
....
343.
      user.setPassword(pwdEncoder.encodePassword(password));
....
345.              return user;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/UnifiedUserAct.java
方法	public String update(Integer id, String email, String password,

```
....
73.         UnifiedUser user = manager.update(id, password, email);
74.         log.info("update UnifiedUser id={}.", user.getId());
```

Side Channel Data Leakage\路径 49:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=49
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	48	70
对象	pass	write

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java
方法	protected void checkUserJson(String username, HttpServletResponse response) {

```
....
48.               pass = "false";
....
52.         ResponseUtils.renderJson(response, pass);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
方法	public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 50:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=50
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	50	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java

方法 protected void checkUserJson(String username, HttpServletResponse response) {

```
....
50.                 pass = manager.usernameNotExist(username) ? "true" :
"false";
....
52.         ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 51:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=51
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	52	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java

方法 protected void checkUserJson(String username, HttpServletResponse response) {

```
....
52.         ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 52:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=52
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	58	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java

方法 protected void checkEmailJson(String email, HttpServletResponse response) {

```
....
58.                 pass = "false";
....
62.         ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 53:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=53
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	60	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java

方法 protected void checkEmailJson(String email, HttpServletResponse response) {

```
....
60.                 pass = manager.emailNotExist(email) ? "true" :
"false";
....
62.         ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 54:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=54
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	62	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsAdminAbstract.java

方法 protected void checkEmailJson(String email, HttpServletResponse response) {

```
....
62.         ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                 String text) {
....
70.                 response.getWriter().write(text);
```

Side Channel Data Leakage\路径 55:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=55
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	141	70
对象	pass	write

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java
方法	public void checkUsername(String username, HttpServletResponse response) {

```
....
141.                    pass = "false";
....
145.              ResponseUtils.renderJson(response, pass);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
方法	public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
方法	public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 56:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathi

	d=56
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	143	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java

方法 public void checkUsername(String username, HttpServletResponse response) {

```
....
143.                    pass = manager.usernameNotExist(username) ?
"true" : "false";
....
145.              ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.          render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 57:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=57
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	145	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsMemberAct.java

方法 public void checkUsername(String username, HttpServletResponse response) {

```
....
145.              ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.          render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 58:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=58

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

行	109	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java

方法 public void checkUserJson(String domain, HttpServletResponse response) {

```
....
109.                    pass = "false";
....
114.              ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.          render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 59:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=59

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	111	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java

方法 public void checkUserJson(String domain, HttpServletResponse response) {

```
....
111.                    pass = manager.findByDomain(domain, false) ==
null ? "true"
....
114.              ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Side Channel Data Leakage\路径 60:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=60

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	114	70
对象	pass	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsSiteAct.java

方法 public void checkUserJson(String domain, HttpServletResponse response) {

```
....
114.                ResponseUtils.renderJson(response, pass);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.    public static void renderJson(HttpServletResponse response, String
text) {
41.            render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.                String text) {
....
70.                response.getWriter().write(text);
```

Side Channel Data Leakage\路径 61:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=61
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	61	446
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount){

```
....
61.   public List<WebpageFavorite> findWebpageFavorite(String
userAccount){
....
64.          query.setString(0, userAccount);
65.          query.setCacheable(false);
66.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount) {

```
....
51.          return WebpageFavoriteDao.findWebpageFavorite(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
445.              List<WebpageFavorite>  list
=WebpageFavoriteMng.findWebpageFavorite(username);
446.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 62:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=62
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	64	446
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount){

```
....
64.          query.setString(0, userAccount);
65.          query.setCacheable(false);
66.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount) {

```
....
51.          return WebpageFavoriteDao.findWebpageFavorite(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
445.              List<WebpageFavorite>  list
=WebpageFavoriteMng.findWebpageFavorite(username);
446.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 63:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=63
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	69	466
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
69.   public List<WebpageFavoritegr> findWebpageFavoriteGr(String
userAccount){
....
72.          query.setString(0, userAccount);
73.          query.setCacheable(false);
74.          return query.list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java
方法	public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
55.          return
WebpageFavoriteDao.findWebpageFavoriteGr(userAccount);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
465.              List<WebpageFavoritegr>  list
=WebpageFavoriteMng.findWebpageFavoriteGr(username);
466.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 64:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=64
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	72	466
对象	userAccount	println

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法	public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
72.          query.setString(0, userAccount);
73.          query.setCacheable(false);
74.          return query.list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java
方法	public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
55.          return
WebpageFavoriteDao.findWebpageFavoriteGr(userAccount);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
方法	public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
465.               List<WebpageFavoritegr>  list
=WebpageFavoriteMng.findWebpageFavoriteGr(username);
466.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 65:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=65
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
行	38	939
对象	userAccount	println

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java

方法 public Pagination getPage(String userAccount,String orderBy, int pageNo, int pageSize,String name){

```
....
38.   public Pagination getPage(String userAccount,String orderBy, int
pageNo, int pageSize,String name){
....
41.         hql.append(userAccount);
42.         hql.append("'");
....
56.         Finder f = Finder.create(hql.toString());
57.         return find(f, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public static Finder create(String hql) {

```
....
31.   public static Finder create(String hql) {
32.         return new Finder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 protected Finder(String hql) {

```
....
23.   protected Finder(String hql) {
24.         hqlBuilder = new StringBuilder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java

方法 public Pagination getPage(String userAccount, String orderBy, int pageNo,

```
....
37.         return WebpageFavoriteDaogr.getPage(userAccount, orderBy,
pageNo, pageSize,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
921.              Pagination pagination =
webpageFavoriteMnggr.getPage(user.getUsername(), orderByFWSC,
cpn(pageNo),5,name);
....
924.              for(int i = 0;i<pagination.getList().size();i++){
....
937.              pagination.setList(listWBF);
....
939.
      System.out.println("js:"+JSONArray.fromObject(pagination).toString
());
```

Side Channel Data Leakage\路径 66:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=66
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
行	41	939
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java

方法 public Pagination getPage(String userAccount,String orderBy, int pageNo, int pageSize,String name){

```
....
41.          hql.append(userAccount);
42.          hql.append("'");
....
56.          Finder f = Finder.create(hql.toString());
57.          return find(f, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public static Finder create(String hql) {

```
....
31.   public static Finder create(String hql) {
32.          return new Finder(hql);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java
方法	protected Finder(String hql) {

```
....
23.   protected Finder(String hql) {
24.         hqlBuilder = new StringBuilder(hql);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java
方法	public Pagination getPage(String userAccount, String orderBy, int pageNo,

```
....
37.         return WebpageFavoriteDaogr.getPage(userAccount, orderBy,
pageNo, pageSize,name);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
方法	public String collection(HttpServletRequest request,

```
....
921.              Pagination pagination =
webpageFavoriteMnggr.getPage(user.getUsername(), orderByFWSC,
cpn(pageNo),5,name);
....
924.              for(int i = 0;i<pagination.getList().size();i++){
....
937.              pagination.setList(listWBF);
....
939.
      System.out.println("js:"+JSONArray.fromObject(pagination).toString
());
```

Side Channel Data Leakage\路径 67:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=67
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageFavoritegr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
行	18	939

对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/WebpageFavoritegr.java

方法 private String userAccount;

```
....
18.   private String userAccount;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
933.                            wf.setDeptname(vp.getDeptname());
934.                            listWBF.add(wf);
....
937.              pagination.setList(listWBF);
....
939.
      System.out.println("js:"+JSONArray.fromObject(pagination).toString
());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/page/Pagination.java

方法 public void setList(List list) {

```
....
78.   public void setList(List list) {
79.         this.list = list;
```

Side Channel Data Leakage\路径 68:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=68
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	49	446
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount) {

```
....
49.   public List<WebpageFavorite> findWebpageFavorite(String
userAccount) {
....
51.         return WebpageFavoriteDao.findWebpageFavorite(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount){

```
....
61.   public List<WebpageFavorite> findWebpageFavorite(String
userAccount){
....
64.         query.setString(0, userAccount);
65.         query.setCacheable(false);
66.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
445.              List<WebpageFavorite>  list
=WebpageFavoriteMng.findWebpageFavorite(username);
446.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 69:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=69
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

行	51	446
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount) {

```
....
51.         return WebpageFavoriteDao.findWebpageFavorite(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavorite> findWebpageFavorite(String userAccount){

```
....
61.   public List<WebpageFavorite> findWebpageFavorite(String
userAccount){
....
64.         query.setString(0, userAccount);
65.         query.setCacheable(false);
66.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
445.              List<WebpageFavorite>  list
=WebpageFavoriteMng.findWebpageFavorite(username);
446.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 70:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=70

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageF	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavori

	avoriteMngImpl.java	teAct.java
行	54	466
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
54.    public List<WebpageFavoritegr> findWebpageFavoriteGr(String
userAccount){
55.          return
WebpageFavoriteDao.findWebpageFavoriteGr(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
69.    public List<WebpageFavoritegr> findWebpageFavoriteGr(String
userAccount){
....
72.          query.setString(0, userAccount);
73.          query.setCacheable(false);
74.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
465.               List<WebpageFavoritegr>  list
=WebpageFavoriteMng.findWebpageFavoriteGr(username);
466.
       System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 71:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=71

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java
行	55	466
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImpl.java

方法 public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
55.         return
WebpageFavoriteDao.findWebpageFavoriteGr(userAccount);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImpl.java

方法 public List<WebpageFavoritegr> findWebpageFavoriteGr(String userAccount){

```
....
69.   public List<WebpageFavoritegr> findWebpageFavoriteGr(String
userAccount){
....
72.         query.setString(0, userAccount);
73.         query.setCacheable(false);
74.         return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/WebpageFavoriteAct.java

方法 public String getFavoriteGrByUser(String username,String areaId,HttpServletRequest request, ModelMap model){

```
....
465.              List<WebpageFavoritegr>  list
=WebpageFavoriteMng.findWebpageFavoriteGr(username);
466.
      System.out.println("JSONArray.fromObject(list).toString():"+JSONAr
ray.fromObject(list).toString());
```

Side Channel Data Leakage\路径 72:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=72

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
行	34	939
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java

方法 public Pagination getPage(String userAccount, String orderBy, int pageNo,

```
....
34.   public Pagination getPage(String userAccount, String orderBy, int
pageNo,
....
37.         return WebpageFavoriteDaogr.getPage(userAccount, orderBy,
pageNo, pageSize,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java

方法 public Pagination getPage(String userAccount,String orderBy, int pageNo, int pageSize,String name){

```
....
38.   public Pagination getPage(String userAccount,String orderBy, int
pageNo, int pageSize,String name){
....
41.         hql.append(userAccount);
42.         hql.append("'");
....
56.         Finder f = Finder.create(hql.toString());
57.         return find(f, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public static Finder create(String hql) {

```
....
31.   public static Finder create(String hql) {
32.         return new Finder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 protected Finder(String hql) {

```
....
23.   protected Finder(String hql) {
24.         hqlBuilder = new StringBuilder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
921.              Pagination pagination =
webpageFavoriteMnggr.getPage(user.getUsername(), orderByFWSC,
cpn(pageNo),5,name);
....
924.              for(int i = 0;i<pagination.getList().size();i++){
....
937.              pagination.setList(listWBF);
....
939.
      System.out.println("js:"+JSONArray.fromObject(pagination).toString
());
```

Side Channel Data Leakage\路径 73:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=73
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java
行	37	939
对象	userAccount	println

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WebpageFavoriteMngImplgr.java

方法 public Pagination getPage(String userAccount, String orderBy, int pageNo,

```
....
37.         return WebpageFavoriteDaogr.getPage(userAccount, orderBy,
pageNo, pageSize,name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WebpageFavoriteDaoImplgr.java

方法 public Pagination getPage(String userAccount,String orderBy, int pageNo, int pageSize,String name){

```
....
38.   public Pagination getPage(String userAccount,String orderBy, int
pageNo, int pageSize,String name){
....
41.         hql.append(userAccount);
42.         hql.append("'");
....
56.         Finder f = Finder.create(hql.toString());
57.         return find(f, pageNo, pageSize);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 public static Finder create(String hql) {

```
....
31.   public static Finder create(String hql) {
32.         return new Finder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/Finder.java

方法 protected Finder(String hql) {

```
....
23.   protected Finder(String hql) {
24.         hqlBuilder = new StringBuilder(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/EnterpriseBanShiTingActgr.java

方法 public String collection(HttpServletRequest request,

```
....
921.              Pagination pagination =
webpageFavoriteMnggr.getPage(user.getUsername(), orderByFWSC,
cpn(pageNo),5,name);
....
924.              for(int i = 0;i<pagination.getList().size();i++){
....
937.              pagination.setList(listWBF);
....
939.
      System.out.println("js:"+JSONArray.fromObject(pagination).toString
());
```

Side Channel Data Leakage\路径 74:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-

	9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=74
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentExt.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java
行	23	187
对象	""author""	info

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/base/BaseContentExt.java

方法 public static String PROP_AUTHOR = "author";

```
....
23.   public static String PROP_AUTHOR = "author";
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/ContributeAct.java

方法 public String save(String title, String author, String description,

```
....
174.              ext.setTitle(title);
175.              ext.setAuthor(author);
176.              ext.setDescription(description);
....
185.              c = contentMng.save(c, ext, t, null, null, null,
tagArr, null, null,
....
187.              log.info("member contribute save Content success.
id={}", c.getId());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/ContentMngImpl.java

方法 public Content save(Content bean, ContentExt ext, ContentTxt txt,

```
....
214.        public Content save(Content bean, ContentExt ext, ContentTxt
txt,
....
241.
      bean.setHasTitleImg(!StringUtils.isBlank(ext.getTitleImg()));
242.              bean.init();
....
259.              bean.addToChannels(channelMng.findById(channelId));
....
274.              bean.setTags(tags);
....
294.              return bean;
```

Reflected XSS All Clients

描述

Reflected XSS All Clients\路径 931:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=931
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	46	64
对象	name	setEncoding

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.              return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                              + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                      Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.          new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                      zipOut = new ZipOutputStream(out);
....
64.                              zipOut.setEncoding(encoding);
```

Reflected XSS All Clients\路径 932:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=932
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	46	73
对象	name	close

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java
方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.                 return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java
方法 public void exportSubmit(HttpServletRequest request,

```
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                                + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.    public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.            new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.    protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                        zipOut = new ZipOutputStream(out);
....
73.                        zipOut.close();
```

Reflected XSS All Clients\路径 933:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=933
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	46	116
对象	name	putNextEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.                 return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                                + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.           new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                       zipOut = new ZipOutputStream(out);
....
69.                             zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
```

Reflected XSS All Clients\路径 934:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=934
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	46	119
对象	name	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.               return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                              + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                      Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                      zipOut = new ZipOutputStream(out);
....
69.                              zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
....
119.                                     zipOut.write(buf, 0, len);
```

Reflected XSS All Clients\路径 935:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=935
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	46	121
对象	name	closeEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
46.                 return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                               + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                       zipOut = new ZipOutputStream(out);
....
69.                             zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
....
121.                                zipOut.closeEntry();
```

Reflected XSS All Clients\路径 936:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=936
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	275	64
对象	request	setEncoding

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
275.        public void exportSubmit(HttpServletRequest request,
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                            + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.               return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
64.                           zipOut.setEncoding(encoding);
```

Reflected XSS All Clients\路径 937:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=937
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	275	73
对象	request	close

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
275.        public void exportSubmit(HttpServletRequest request,
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                            + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.                return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
73.                     zipOut.close();
```

Reflected XSS All Clients\路径 938:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=938

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	275	116
对象	request	putNextEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
275.        public void exportSubmit(HttpServletRequest request,
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                            + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.               return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法	protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                       zipOut = new ZipOutputStream(out);
....
69.                             zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
方法	private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
```

Reflected XSS All Clients\路径 939:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=939
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	275	119
对象	request	write

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java
方法	public void exportSubmit(HttpServletRequest request,

```
....
275.        public void exportSubmit(HttpServletRequest request,
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                            + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.                return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
69.                           zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                    zipOut.putNextEntry(entry);
....
119.                                          zipOut.write(buf, 0, len);
```

Reflected XSS All Clients\路径 940:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=940
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	275	121
对象	request	closeEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
275.        public void exportSubmit(HttpServletRequest request,
....
277.                String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                            + solution + ".zip");
....
281.                response.addHeader("Content-disposition",
"filename=template-"
....
285.                        Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
41.   public static String getQueryParam(HttpServletRequest request,
String name) {
....
45.         if (request.getMethod().equalsIgnoreCase(POST)) {
46.               return request.getParameter(name);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
69.                           zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
....
121.                                zipOut.closeEntry();
```

Reflected XSS All Clients\路径 941:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=941
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	48	64
对象	getQueryString	setEncoding

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
140.                    if (ht.containsKey(key)) {
141.                          String oldVals[] = (String[]) ht.get(key);
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                          + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                    Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.          new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
64.                           zipOut.setEncoding(encoding);
```

Reflected XSS All Clients\路径 942:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=942
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	48	73
对象	getQueryString	close

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.          String s = request.getQueryString();
....
53.                s = URLDecoder.decode(s, UTF8);
....
57.          String[] values = parseQueryString(s).get(name);
....
59.                return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
140.                    if (ht.containsKey(key)) {
141.                          String oldVals[] = (String[]) ht.get(key);
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                          + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                    Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                   zipOut = new ZipOutputStream(out);
....
73.                   zipOut.close();
```

Reflected XSS All Clients\路径 943:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=943
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	48	116
对象	getQueryString	putNextEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
140.                    if (ht.containsKey(key)) {
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                              + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                      Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.          new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                      zipOut = new ZipOutputStream(out);
....
69.                              zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
```

Reflected XSS All Clients\路径 944:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=944
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	48	119
对象	getQueryString	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                          + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                    Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                     zipOut = new ZipOutputStream(out);
....
69.                           zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
....
119.                                      zipOut.write(buf, 0, len);
```

Reflected XSS All Clients\路径 945:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=945
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	48	121
对象	getQueryString	closeEntry

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static String getQueryParam(HttpServletRequest request, String name) {

```
....
48.         String s = request.getQueryString();
....
53.               s = URLDecoder.decode(s, UTF8);
....
57.         String[] values = parseQueryString(s).get(name);
....
59.               return values[values.length - 1];
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/RequestUtils.java

方法 public static Map<String, String[]> parseQueryString(String s) {

```
....
125.        public static Map<String, String[]> parseQueryString(String
s) {
....
131.              StringTokenizer st = new StringTokenizer(s, "&");
132.              while (st.hasMoreTokens()) {
133.                    String pair = (String) st.nextToken();
134.                    int pos = pair.indexOf('=');
....
138.                    String key = pair.substring(0, pos);
....
151.                    ht.put(key, valArray);
....
153.              return ht;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/assist/TemplateAct.java

方法 public void exportSubmit(HttpServletRequest request,

```
....
277.              String solution = RequestUtils.getQueryParam(request,
"solution");
....
282.                          + solution + ".zip");
....
281.              response.addHeader("Content-disposition",
"filename=template-"
....
285.                    Zipper.zip(response.getOutputStream(),
fileEntrys, "GBK");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 public static void zip(OutputStream out, List<FileEntry> fileEntrys,

```
....
31.   public static void zip(OutputStream out, List<FileEntry>
fileEntrys,
....
33.         new Zipper(out, fileEntrys, encoding);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 protected Zipper(OutputStream out, List<FileEntry> fileEntrys,

```
....
54.   protected Zipper(OutputStream out, List<FileEntry> fileEntrys,
....
61.                       zipOut = new ZipOutputStream(out);
....
69.                             zip(fe.getFile(), fe.getFilter(),
fe.getZipEntry(), fe
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
116.                                zipOut.putNextEntry(entry);
....
121.                                zipOut.closeEntry();
```

Reflected XSS All Clients\路径 946:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=946
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp
行	42	41
对象	getValue	println

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp

方法 <%@ page contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"

```
....
42.                                 + cookies[i].getValue() + "]");
....
41.                       out.println(cookies[i].getName() + "=["
```

Reflected XSS All Clients\路径 947:

严重程度： 高风险
结果状态： 等待确认

在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=947
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp
行	38	41
对象	getCookies	println

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp

方法 <%@ page contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"

```
....
38.         Cookie[] cookies = request.getCookies();
....
42.                                     + cookies[i].getValue() + "]");
....
41.                     out.println(cookies[i].getName() + "=["
```

Reflected XSS All Clients\路径 948:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=948
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp	/WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp
行	41	41
对象	getName	println

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/WEB-INF/error/uncaught_exception.jsp

方法 <%@ page contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"

```
....
41.                     out.println(cookies[i].getName() + "=["
```

Reflected XSS All Clients\路径 949:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=949
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	307	321
对象	sxid	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
312.                        xml =
matterService.getFormInfoXml(sxid,groupid);
....
321.                out.print(xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
41.   public String getFormInfoXml(String sxid, String groupid) {
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
43.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
660.        public String getFormInfoXml(String sxid, String groupid) {
....
683.                    xml.append("<sxid>"+sxid+"</sxid>");
684.                    xml.append("<ctype>1</ctype>");
685.                    xml.append("<templateid></templateid>");
686.                    xml.append("<templateName></templateName>");
687.                    xml.append("<bz></bz>");
688.                    xml.append("<cclid></cclid>");
689.                    xml.append("<fname></fname>");
690.                    xml.append("<orinum></orinum>");
691.                    xml.append("<copynum></copynum>");
692.                    xml.append("<pid></pid>");
693.                    xml.append("<clbh></clbh>");
....
711.                    xml.append("</form>\n");
....
796.                xml.append("<length>"+i+"</length>");
797.                xml.append("</formlist>");
798.                return xml.toString();
```

Reflected XSS All Clients\路径 950:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=950
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	307	321
对象	bsid	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
307.        public String form(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
316.                    xml = matterService.getFormInfoXml(bsid);
....
321.                out.print(xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
59.   public String getFormInfoXml(String bsid) throws Exception{
60.         String xml = this.matterDao.getFormInfoXml(bsid);
61.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
802.        public String getFormInfoXml(String bsid) throws Exception{
....
839.              TInsWebhallBusinessInfo info =
(TInsWebhallBusinessInfo)this.getSession().get(TInsWebhallBusinessInfo.c
lass, bsid);
....
854.                    xml.append("<sxid>"+info.getPid()+"-
"+info.getItemid()+"</sxid>");
855.                    xml.append("<ctype>"+sb.getStatus()+"</ctype>");
856.                    xml.append("<templateid></templateid>");
857.                    xml.append("<templateName></templateName>");
858.                    xml.append("<bz></bz>");
859.                    xml.append("<cclid>"+sb.getClid()+"</cclid>");
860.                    xml.append("<fname>"+sb.getClmc()+"</fname>");
....
862.
      xml.append("<orinum>"+clxx.getOrinum()+"</orinum>");
863.
      xml.append("<copynum>"+clxx.getCopynum()+"</copynum>");
864.                    xml.append("<pid></pid>");
865.                    xml.append("<clbh>"+clxx.getClbh()+"</clbh>");
866.                    xml.append("</form>\n");
....
869.              xml.append("<length>"+i+"</length>");
870.              xml.append("</formlist>");
871.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsWebhallBusinessInfo.java

方法 public String getItemid() {

```
....
128.              return itemid;
```

Reflected XSS All Clients\路径 951:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=951
结果评论
被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	328	341
对象	sxid	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
....
341.              out.print(xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
45.   public String getFormInfoHtmlXml(String sxid,String groupid,String
userid) {
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
47.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
132.        public String getFormInfoHtmlXml(String sxid,String
groupid,String userid){
....
181.                    xml.append("<sxid>"+sxid+"</sxid>");
182.                    xml.append("<ctype>1</ctype>");
183.                    xml.append("<templateid></templateid>");
184.                    xml.append("<templateName></templateName>");
185.                    xml.append("<bz></bz>");
186.                    xml.append("<cclid></cclid>");
187.                    xml.append("<fname></fname>");
188.                    xml.append("<orinum></orinum>");
189.                    xml.append("<copynum></copynum>");
190.                    xml.append("<pid></pid>");
191.                    xml.append("<clbh></clbh>");
....
197.                    xml.append(html);
....
199.                    xml.append("</form>\n");
....
248.            xml.append("<length>" + i + "</length>");
249.            xml.append("</formlist>");
....
251.            return xml.toString();
```

Reflected XSS All Clients\路径 952:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=952
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	328	341
对象	bsid	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
328.        public String formHtml(String sxid,String groupid,String
bsid, HttpServletRequest request,
....
336.                    xml = matterService.getFormInfoHtmlXml(bsid);
....
341.            out.print(xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
50.   public String getFormInfoHtmlXml(String bsid) throws Exception{
51.         String xml = this.matterDao.getFormInfoHtmlXml(bsid);
52.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
342.        public String getFormInfoHtmlXml(String bsid) throws
Exception{
....
392.              TInsWebhallBusinessInfo info =
(TInsWebhallBusinessInfo)this.getSession().get(TInsWebhallBusinessInfo.c
lass, bsid);
....
407.                    xml.append("<sxid>"+info.getPid()+"-
"+info.getItemid()+"</sxid>");
408.                    xml.append("<ctype>"+sb.getStatus()+"</ctype>");
409.                    xml.append("<templateid></templateid>");
410.                    xml.append("<templateName></templateName>");
411.                    xml.append("<bz></bz>");
412.                    xml.append("<cclid>"+sb.getClid()+"</cclid>");
413.                    xml.append("<fname>"+sb.getClmc()+"</fname>");
....
415.
      xml.append("<orinum>"+clxx.getOrinum()+"</orinum>");
416.
      xml.append("<copynum>"+clxx.getCopynum()+"</copynum>");
417.                    xml.append("<pid></pid>");
418.                    xml.append("<clbh>"+clxx.getClbh()+"</clbh>");
419.                    xml.append("<xml><![CDATA[");
....
426.                    xml.append("]]></xml>");
427.                    xml.append("<formhtmldata><![CDATA[");
428.                    xml.append(getFormInfoHtmlData(null, null,
insformdata
....
430.                    xml.append("]]></formhtmldata>");
431.                    xml.append("</form>\n");
....
434.              xml.append("<length>"+i+"</length>");
435.              xml.append("</formlist>");
436.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsWebhallBusinessInfo.java

方法 public String getItemid() {

```
....
128.              return itemid;
```

Reflected XSS All Clients\路径 953:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=953
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	348	362
对象	bsid	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String wssbForm(String sxid,String formid,String formver,String groupid,String bsid, HttpServletRequest request,

```
....
348.        public String wssbForm(String sxid,String formid,String
formver,String groupid,String bsid, HttpServletRequest request,
....
357.                    xml = matterService.getFormInfoXml(bsid);
....
362.              out.print(xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
59.   public String getFormInfoXml(String bsid) throws Exception{
60.         String xml = this.matterDao.getFormInfoXml(bsid);
61.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String bsid) throws Exception{

```
....
802.        public String getFormInfoXml(String bsid) throws Exception{
....
839.              TInsWebhallBusinessInfo info =
(TInsWebhallBusinessInfo)this.getSession().get(TInsWebhallBusinessInfo.c
lass, bsid);
....
854.                    xml.append("<sxid>"+info.getPid()+"-
"+info.getItemid()+"</sxid>");
855.                    xml.append("<ctype>"+sb.getStatus()+"</ctype>");
856.                    xml.append("<templateid></templateid>");
857.                    xml.append("<templateName></templateName>");
858.                    xml.append("<bz></bz>");
859.                    xml.append("<cclid>"+sb.getClid()+"</cclid>");
860.                    xml.append("<fname>"+sb.getClmc()+"</fname>");
....
862.
      xml.append("<orinum>"+clxx.getOrinum()+"</orinum>");
863.
      xml.append("<copynum>"+clxx.getCopynum()+"</copynum>");
864.                    xml.append("<pid></pid>");
865.                    xml.append("<clbh>"+clxx.getClbh()+"</clbh>");
866.                    xml.append("</form>\n");
....
869.              xml.append("<length>"+i+"</length>");
870.              xml.append("</formlist>");
871.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsWebhallBusinessInfo.java

方法 public String getItemid() {

```
....
128.              return itemid;
```

Reflected XSS All Clients\路径 954:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=954
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	369	392
对象	sxid	print

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
369.        public String cl(String sxid,String groupid,String bsid,
HttpServletRequest request,
....
375.                    xml = matterService.getClXml(sxid,groupid);
....
392.              out.print(xml);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getClXml(String sxid,String groupid) {

```
....
30.   public String getClXml(String sxid,String groupid) {
31.         String xml = this.matterDao.getClXml(sxid, groupid);
32.         return xml;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXml(String sxid,String groupid) {

```
....
43.   public String getClXml(String sxid,String groupid) {
....
108.                    xml.append("<sxid>"+sxid+"</sxid>");
109.                    xml.append("<ctype></ctype>");
110.                    xml.append("<templateid></templateid>");
111.                    xml.append("<templateName></templateName>");
112.                    xml.append("<bz>"+temp[14]+"</bz>");//存放
T_END_SD_CLNR 备注字段
113.
      xml.append("<cclid>"+changeStr(temp[0].toString())+"</cclid>");
114.
      xml.append("<fname>"+changeStr(temp[1].toString())+"</fname>");
115.
      xml.append("<orinum>"+changeStr((temp[8]==null?"":temp[8].toString
()))+"</orinum>");
116.
      xml.append("<copynum>"+changeStr((temp[9]==null?"":temp[9].toStrin
g()))+"</copynum>");
117.                    xml.append("<pid></pid>");
118.
      xml.append("<clbh>"+changeStr((temp[10]==null?"":temp[10].toString
()))+"</clbh>");
....
120.
      xml.append("<sfby>"+((temp[11]+"").equals("1")?"1":"0")+"</sfby>")
;
....
123.                    xml.append("<yq>"+temp[12]+"</yq>");//存放
T_END_SD_CLNR 要求字段
124.
      xml.append("<zzhdzh>"+temp[13]+"</zzhdzh>");//存放 T_END_SD_CLNR
资质或者电子化字段
125.                    xml.append("</cl>\n");
....
128.              xml.append("<length>"+i+"</length>");
129.              xml.append("</cllist>");
130.              return xml.toString();
```

Reflected XSS All Clients\路径 955:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=955
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	144	775
对象	""promise_value""	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String saveOrUpdate(String xmlStr,

```
....
144.                            dataxml=ywpzGenerator(insbusi, xmlStr
,request.getParameter("promise_value"));// 0708注销
....
163.              return dataxml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 private String ywpzGenerator(TInsWebhallBusinessInfo insbusi, String xmlStr,String promise_value)

```
....
514.        private String ywpzGenerator(TInsWebhallBusinessInfo
insbusi, String xmlStr,String promise_value)
....
546.
      dataXml.append("<promisedata>"+promise_value+"</promisedata>\n");
547.                    dataXml.append("<clxxs>\n");// 材料清单-开始
....
584.                    dataXml.append("</clxxs>\n");// 材料清单-结束
585.                    dataXml.append("</data>");
....
591.                    oneYwpz.setDataXml(dataXml.toString());
....
594.              return dataXml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String sbsubmit(String cllist,String formlist,String poststr, HttpServletRequest request,

```
....
751.              String sqpz_xml=wssbService.saveOrUpdate(cllist,
flist, AREAID ,request);
....
775.              out.print(sqpz_xml);
```

Reflected XSS All Clients\路径 956:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=956

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	713	775
对象	request	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String sbsubmit(String cllist,String formlist,String poststr, HttpServletRequest request,

```
....
713.        public String sbsubmit(String cllist,String formlist,String
poststr, HttpServletRequest request,
....
751.                String sqpz_xml=wssbService.saveOrUpdate(cllist,
flist, AREAID ,request);
....
775.                out.print(sqpz_xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String saveOrUpdate(String xmlStr,

```
....
118.                    ArrayList<FormPropertyVo> formPropList, String
preposeFlag,HttpServletRequest request)
....
144.                            dataxml=ywpzGenerator(insbusi, xmlStr
,request.getParameter("promise_value"));// 0708注销
....
163.                return dataxml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 private String ywpzGenerator(TInsWebhallBusinessInfo insbusi, String xmlStr,String promise_value)

```
....
514.        private String ywpzGenerator(TInsWebhallBusinessInfo
insbusi, String xmlStr,String promise_value)
....
546.
      dataXml.append("<promisedata>"+promise_value+"</promisedata>\n");
547.                    dataXml.append("<clxxs>\n");// 材料清单-开始
....
584.                    dataXml.append("</clxxs>\n");// 材料清单-结束
585.                    dataXml.append("</data>");
....
591.                    oneYwpz.setDataXml(dataXml.toString());
....
594.              return dataXml.toString();
```

Reflected XSS All Clients\路径 957:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=957
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	713	775
对象	cllist	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String sbsubmit(String cllist,String formlist,String poststr, HttpServletRequest request,

```
....
713.        public String sbsubmit(String cllist,String formlist,String
poststr, HttpServletRequest request,
....
751.              String sqpz_xml=wssbService.saveOrUpdate(cllist,
flist, AREAID ,request);
....
775.              out.print(sqpz_xml);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String saveOrUpdate(String xmlStr,

```
....
117.        public String saveOrUpdate(String xmlStr,
....
144.                            dataxml=ywpzGenerator(insbusi, xmlStr
,request.getParameter("promise_value"));// 0708注销
....
163.              return dataxml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 private String ywpzGenerator(TInsWebhallBusinessInfo insbusi, String xmlStr,String promise_value)

```
....
514.        private String ywpzGenerator(TInsWebhallBusinessInfo
insbusi, String xmlStr,String promise_value)
....
518.              StringReader reader = new StringReader(xmlStr);
519.              InputSource source = new InputSource(reader);
520.              org.w3c.dom.Document document = db.parse(source);
521.              NodeList cNodeList =
document.getElementsByTagName("cl");
....
549.                    for (int i = 0; i < cNodeList.getLength(); i++)
{
550.                            org.w3c.dom.Element dataNode =
(org.w3c.dom.Element) cNodeList.item(i);
551.                            String no =
dataNode.getAttributes().getNamedItem("no").getNodeValue();
552.                            String clmc =
dataNode.getAttributes().getNamedItem("clmc").getNodeValue();
....
569.                                  dataXml.append("<clmc>" + clmc +
"</clmc>\n");// 材料名称
570.                                  dataXml.append("<tjfs>" + dzhyqName
+ "</tjfs>\n");// 电子化上传类型
571.                                  dataXml.append("<bz>" + clbz +
"</bz>\n");// 备注
572.                                  dataXml.append("</clxx>\n");
....
584.                    dataXml.append("</clxxs>\n");// 材料清单-结束
585.                    dataXml.append("</data>");
....
591.                    oneYwpz.setDataXml(dataXml.toString());
....
594.              return dataXml.toString();
```

Reflected XSS All Clients\路径 958:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=958
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java
行	131	510
对象	""fileid""	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/UploadFileServlet.java

方法 public void doPost(HttpServletRequest request, HttpServletResponse response)

```
....
131.                    String fileId = request.getParameter("fileid");
....
159.                                    result =
mongoFile.saveFile(fileId,fileName,item, null);
....
510.              out.print(result);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/MongoFile.java

方法 public String saveFile(String fileid,String name,InputStream inputStream, Map<String, Object> param)

```
....
109.        public String saveFile(String fileid,String name,InputStream
inputStream, Map<String, Object> param)
....
126.              return fileid;
```

Reflected XSS All Clients\路径 959:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=959

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	39	70
对象	captcha	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Captcha.java

方法 public void doSyncValidate(HttpServletRequest request,HttpServletResponse response, String captcha){

```
....
39.   public void doSyncValidate(HttpServletRequest
request,HttpServletResponse response, String captcha){
....
45.                       rStr  += captcha;
....
54.                       json.put("valivalue", rStr);
55.                       ResponseUtils.renderJson(response,
json.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.          render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Reflected XSS All Clients\路径 960:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=960
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RestTestService.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RestTestService.java
行	49	52
对象	id	id

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/RestTestService.java

方法 public String test(@PathParam("id")

```
....
49.    String id) throws Exception {
....
52.                 return id;
```

Reflected XSS All Clients\路径 961:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=961
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java
行	185	258
对象	""fileNo""	setCharacterEncoding

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java

方法 public void doPost(HttpServletRequest request, HttpServletResponse response)

```
....
185.              String fileId = request.getParameter("fileNo");
....
244.                           map.put("fileid", fileId);
....
247.                                 db = mongoFile.findFile(map);
....
254.                                       + new
String(db.getFilename().getBytes("gb2312"),
....
253.                           response.addHeader("Content-Disposition",
"attachment; filename=\""
....
256.                           response.setHeader("Content-Length",
String.valueOf(db
....
258.                           response.setCharacterEncoding("utf-8");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/MongoFile.java

方法 public GridFSDBFile findFile(Map<String, Object> param) throws Exception {

```
....
29.   public GridFSDBFile findFile(Map<String, Object> param) throws
Exception {
....
38.         obj.putAll(param);
....
40.         GridFSDBFile flout = f.findOne(obj);
41.         return flout;
```

Reflected XSS All Clients\路径 962:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=962
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java
行	185	364
对象	""fileNo""	setCharacterEncoding

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/servlet/DownloadFileServlet.java

方法 public void doPost(HttpServletRequest request, HttpServletResponse response)

```
....
185.              String fileId = request.getParameter("fileNo");
....
350.                           map.put("fileid", fileId);
....
353.                                 db = mongoFileQzqd.findFile(map);
....
360.                                       + new
String(db.getFilename().getBytes("gb2312"),
....
359.                           response.addHeader("Content-Disposition",
"attachment; filename=\""
....
362.                           response.setHeader("Content-Length",
String.valueOf(db
....
364.                           response.setCharacterEncoding("utf-8");
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/upload/MongoFileQzqd.java

方法 public GridFSDBFile findFile(Map<String, Object> param) throws Exception {

```
....
31.   public GridFSDBFile findFile(Map<String, Object> param) throws
Exception {
....
40.          obj.putAll(param);
....
42.          GridFSDBFile flout = f.findOne(obj);
43.          return flout;
```

Stored XSS

描述

Stored XSS\路径 3362:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3362
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
行	58	769
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getListByAreaid(String areaid) {

```
....
58.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java

方法 public List<SysRegion> getListByAreaid(String areaid) {

```
....
67.          return dao.getListByAreaid(areaid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java

方法 public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
698.              List<SysRegion> sysRegions =
sysRegionMng.getListByAreaid(areaId);
....
703.                  areaids.add(region.getAreaid());
....
706.                  object.put("pId", region.getAreaid());
707.                  object.put("name", region.getName());
708.                  object.put("issystem", "true");// 是否有子菜单
709.                  object.put("open", "true");// 默认是否展开
710.                  object.put("children", array);
....
712.                  objmap.put(region.getAreaid(), object);
....
752.              parentArray.add(objmap.get(areaId));
....
769.                  out.print(parentArray);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java

方法 public String getName() {

```
....
33.         return name;
```

Stored XSS\路径 3363:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3363
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
行	58	767
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsSysRegionDaoImpl.java

方法 public List<SysRegion> getListByAreaid(String areaid) {

```
....
58.          return query.list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SysRegionMngImpl.java
方法	public List<SysRegion> getListByAreaid(String areaid) {

```
....
67.          return dao.getListByAreaid(areaid);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/member/SpaceAct.java
方法	public String spacedeptlist(String areaId, String type, HttpServletRequest request, HttpServletResponse response,

```
....
698.              List<SysRegion> sysRegions =
sysRegionMng.getListByAreaid(areaId);
....
703.                  areaids.add(region.getAareaid());
....
706.                  object.put("pId", region.getAareaid());
707.                  object.put("name", region.getName());
708.                  object.put("issystem", "true");// 是否有子菜单
709.                  object.put("open", "true");// 默认是否展开
710.                  object.put("children", array);
....
712.                  objmap.put(region.getAareaid(), object);
....
752.              parentArray.add(objmap.get(areaId));
....
766.                  outArray.addAll(parentArray);
767.                  out.print(outArray);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SysRegion.java
方法	public String getName() {

```
....
33.          return name;
```

Stored XSS\路径 3364:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3364
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

行	87	392
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getClXml(String sxid,String groupid) {

```
....
87.         for(Object o:
getSession().createSQLQuery(sql.toString()).list()){
....
113.
      xml.append("<cclid>"+changeStr(temp[0].toString())+"</cclid>");
....
124.
      xml.append("<zzhdzh>"+temp[13]+"</zzhdzh>");//存放 T_END_SD_CLNR
资质或者电子化字段
125.                    xml.append("</cl>\n");
....
128.              xml.append("<length>"+i+"</length>");
129.              xml.append("</cllist>");
130.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String sxid,String groupid) {

```
....
31.         String xml = this.matterDao.getClXml(sxid, groupid);
32.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
375.                    xml = matterService.getClXml(sxid,groupid);
....
392.              out.print(xml);
```

Stored XSS\路径 3365:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3365
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	208	341
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
208.        for (Object o :
this.getSession().createSQLQuery(sql).list()) {
....
219.
      xml.append("<formver>"+temp[6].toString()+"</formver>");
220.              xml.append("<uid></uid>");
221.              xml.append("<fid>"+gid+"</fid>");
222.              xml.append("<zt></zt>");
223.              xml.append("<sxid>"+sxid+"</sxid>");
224.              xml.append("<ctype>1</ctype>");
225.              xml.append("<templateid></templateid>");
226.              xml.append("<templateName></templateName>");
227.              xml.append("<bz></bz>");
228.              xml.append("<cclid></cclid>");
229.              xml.append("<fname></fname>");
230.              xml.append("<orinum></orinum>");
231.              xml.append("<copynum></copynum>");
232.              xml.append("<pid></pid>");
233.              xml.append("<clbh></clbh>");
....
241.              xml.append(html);
....
244.              xml.append("</form>");
....
248.              xml.append("<length>" + i + "</length>");
249.              xml.append("</formlist>");
....
251.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
47.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法	public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
....
341.              out.print(xml);
```

Stored XSS\路径 3366:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3366
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	511	392
对象	list	print

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXml(String bsid) throws Exception{

```
....
511.              for(Object
sb:this.getSession().createSQLQuery(sql.toString()).list()){
....
524.
      xml.append("<gid>"+changeStr(temp[3].toString())+"</gid>");
....
540.
      xml.append("<uid>"+changeStr(temp[6].toString())+"</uid>");
....
602.
      xml.append("<cclid>"+changeStr(temp[0].toString())+"</cclid>");
....
609.                    if((temp[8]!= null && !temp[8].equals("")) &&
....
612.                            String[] fids =
temp[8].toString().split(";");
613.                            String[] fnames =
temp[9].toString().split(";");
....
615.                                    filelist +=
fids[j]+":"+(fnames[j]==null?"":fnames[j])+";";
....
617.
      xml.append("<filelist>"+filelist+"</filelist>");
....
619.                            xml.append("<xid>"+fids[fids.length-
1]+"</xid>");
620.                            xml.append("<fid>"+fids[fids.length-
1]+"</fid>");
....
626.                    xml.append("</cl>\n");
....
629.              xml.append("<length>"+i+"</length>");
....
631.              xml.append("<sxname><![CDATA["+(p ==
null?"":CTools.getEndStr(p.getSxzxname(),"&&"))+"]]></sxname>");
632.              xml.append("</cllist>");
633.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
37.         String xml = this.matterDao.getClXml(bsid);
38.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
377.                    xml = matterService.getClXml(bsid);
....
392.              out.print(xml);
```

Stored XSS\路径 3367:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3367
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	570	392
对象	list	print

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getClXml(String bsid) throws Exception{

```
....
570.                                List list =
getSession().createSQLQuery(sql2).list();
....
572.                                if(list!=null && list.size()!=0){
573.                                      sfby = list.get(0)+"";
....
575.
      xml.append("<sfby>"+changeStr(sfby)+"</sfby>");
....
593.
      xml.append("<sxid>"+changeStr(p.getId())+"</sxid>");
....
598.                    xml.append("<ctype>"+temp_3+"</ctype>");
599.                    xml.append("<templateid></templateid>");
600.                    xml.append("<templateName></templateName>");
601.                    xml.append("<bz>"+temp[11]+"</bz>");
602.
      xml.append("<cclid>"+changeStr(temp[0].toString())+"</cclid>");
603.
      xml.append("<fname>"+changeStr(temp[1].toString())+"</fname>");
....
605.
      xml.append("<orinum>"+clxx.getOrinum()+"</orinum>");
606.
      xml.append("<copynum>"+clxx.getCopynum()+"</copynum>");
607.                    xml.append("<pid></pid>");
608.
      xml.append("<clbh>"+changeStr(clxx.getClbh())+"</clbh>");
....
622.                            xml.append("<filelist></filelist>");
623.                            xml.append("<xid></xid>");
624.                            xml.append("<fid></fid>");
....
626.                    xml.append("</cl>\n");
....
629.              xml.append("<length>"+i+"</length>");
....
631.              xml.append("<sxname><![CDATA["+(p ==
null?"":CTools.getEndStr(p.getSxzxname(),"&&"))+"]]></sxname>");
632.              xml.append("</cllist>");
633.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 private String changeStr(String v){

```
....
636.        private String changeStr(String v){
637.              String result = v;
638.              if(result.indexOf("<<")>-1){
....
641.              if(result.indexOf(">>")>-1){
....
644.              if(result.indexOf("<")>-1){
....
647.              if(result.indexOf(">")>-1){
....
650.              if(result.indexOf("》")>-1){
....
653.              if(result.indexOf("《")>-1){
....
657.              return result;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getClXml(String bsid) throws Exception{

```
....
37.         String xml = this.matterDao.getClXml(bsid);
38.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String cl(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
377.                    xml = matterService.getClXml(bsid);
....
392.              out.print(xml);
```

Stored XSS\路径 3368:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3368
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	764	321

对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
764.              for(Object o:
this.getSession().createSQLQuery(sql).list()){
....
787.
      xml.append("<fname>"+temp[1].toString()+"</fname>");
....
789.
      xml.append("<orinum>"+clxx.getOrinum()+"</orinum>");
790.
      xml.append("<copynum>"+clxx.getCopynum()+"</copynum>");
791.                    xml.append("<pid></pid>");
792.                    xml.append("<clbh>"+clxx.getClbh()+"</clbh>");
793.                    xml.append("</form>\n");
....
796.              xml.append("<length>"+i+"</length>");
797.              xml.append("</formlist>");
798.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
43.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
312.                    xml =
matterService.getFormInfoXml(sxid,groupid);
....
321.              out.print(xml);
```

Stored XSS\路径 3369:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3369
结果评论	
被分配给	

状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	880	299
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getGroupXml(String sxid) throws Exception {

```
....
880.              for(Object o:
this.getSession().createSQLQuery(sql).list()){
....
884.
      xml.append("<name>"+temp[1].toString()+"</name>");
885.                    xml.append("</group>\n");
....
888.              xml.append("<length>"+i+"</length>");
....
929.              xml.append("<tempid>"+bsnum+"</tempid>");
....
933.
      xml.append("<sxname><![CDATA["+CTools.getEndStr(p.getSxzxname(),"&
&")+"]]></sxname>");
934.              xml.append("</grouplist>");
935.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getGroupXml(String sxid) throws Exception {

```
....
65.         String xml = this.matterDao.getGroupXml(sxid);
66.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String clxxgroup(String sxid, HttpServletRequest request,

```
....
295.                    String xml=matterService.getGroupXml(sxid);
....
299.                    out.print(xml);
```

Stored XSS\路径 3370:

严重程度：	高风险

结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3370
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceAttachBaseDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	129	611
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceAttachBaseDaoImpl.java

方法 public List<SpaceAttachBase> findByAttachCode(String attachCode) {

```
....
129.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceAttachBaseMngImpl.java

方法 public List<SpaceAttachBase> findByAttachCode(String attachCode) {

```
....
57.         return dao.findByAttachCode(attachCode);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getkonjianfj(String fileid, HttpServletRequest request,

```
....
601.              List<SpaceAttachBase> attachs =
attachBaseMng.findByAttachCode("201512221805201000");
....
606.                    cl.append("<fjid>"+t.getId()+"</clid>");
607.
      cl.append("<fjname>"+t.getAttachName()+"</filename>");
608.                    cl.append("</clMess>");
....
610.              cl.append("</cl>");
611.              out.print(cl.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceAttachBase.java

方法	public String getAttachName() {

```
....
91.         return this.attachName;
```

Stored XSS\路径 3371:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3371
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceClxxInfoDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	147	587
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/SpaceClxxInfoDaoImpl.java

方法 public List<SpaceClxxInfo> findByUserCode(String inczzjgdm) {

```
....
147.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/SpaceClxxInfoMngImpl.java

方法 public List<SpaceClxxInfo> findByUserCode(String inczzjgdm) {

```
....
32.         return dao.findByUserCode( inczzjgdm);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getkonjiancl(String utype, String uid,String clid, HttpServletRequest request,

```
....
551.              List<SpaceClxxInfo> clxx =
spaceClxxMng.findByUserCode(usercode);
....
556.                    cl.append("<clid>"+t.getId()+"</clid>");
557.
      cl.append("<filename>"+t.getClmc()+"</filename>");
558.                    cl.append("</clMess>");
....
586.              cl.append("</cl>");
587.              out.print(cl.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/SpaceClxxInfo.java

方法 public String getClmc() {

```
....
90.          return this.clmc;
```

Stored XSS\路径 3372:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3372
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java
行	47	112
对象	list	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TInsAdviceDaoImpl.java

方法 public List<TInsAdvice> findByBsnum(String bsnum){

```
....
47.          return query.list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsAdviceServiceImpl.java

方法 public List<TInsAdvice> findByBsnum(String bsnum){

```
....
35.          return this.dao.findByBsnum(bsnum);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/InsAdviceAct.java

方法 public void preCounsel2(HttpServletRequest request,HttpServletResponse response, ModelMap model) throws Exception {

```
....
110.                    List<TInsAdvice> list =
this.tInsAdviceService.findByBsnum(bid);
....
112.
      response.getWriter().write("|"+JSONObject.fromObject(list.get(0)).
toString());
```

Stored XSS\路径 3373:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3373
结果评论
被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	141	775
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/WssbDAOImp.java

方法 public String getClBzInfo(String clid){

```
....
141.              clbz = query.list().get(0).toString();
....
145.        return clbz;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getClBz(String clid) {

```
....
706.              return wssbDao.getClBzInfo(clid);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 private String ywpzGenerator(TInsWebhallBusinessInfo insbusi, String xmlStr,String promise_value)

```
....
555.                            String clbz = this.getClBz(clid);
....
579.                                  dataXml.append("<bz>" + clbz +
"</bz>\n");// 备注
580.                                  dataXml.append("</clxx>\n");
....
584.                      dataXml.append("</clxxs>\n");// 材料清单-结束
585.                      dataXml.append("</data>");
....
591.                      oneYwpz.setDataXml(dataXml.toString());
....
594.              return dataXml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String saveOrUpdate(String xmlStr,

```
....
144.                            dataxml=ywpzGenerator(insbusi, xmlStr
,request.getParameter("promise_value"));// 0708注销
....
163.              return dataxml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String sbsubmit(String cllist,String formlist,String poststr, HttpServletRequest request,

```
....
751.              String sqpz_xml=wssbService.saveOrUpdate(cllist,
flist, AREAID ,request);
....
775.              out.print(sqpz_xml);
```

Stored XSS\路径 3374:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3374
结果评论

被分配给
状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	51	70
对象	list	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsTopicDaoImpl.java

方法 public List<CmsTopic> getGlobalTopicList() {

```
....
70.         return find(hql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsTopicMngImpl.java

方法 public List<CmsTopic> getListByChannel(Integer channelId) {

```
....
41.         List<CmsTopic> list = dao.getGlobalTopicList();
....
44.         return list;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsTopicAct.java

方法 public void topicsByChannel(Integer channelId, HttpServletResponse response)

```
....
163.                    List<CmsTopic> list =
manager.getListByChannel(channelId);
....
165.                    for (CmsTopic t : list) {
....
167.                          o.put("id", t.getId());
168.                          o.put("name", t.getName());
169.                          arr.put(o);
....
172.              ResponseUtils.renderJson(response, arr.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.          render(response, "application/json;charset=UTF-8", text);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java

方法 public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Stored XSS\路径 3375:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3375
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	51	321
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoXml(String sxid, String groupid) {

```
....
665.              List<TSysFlowlibmapform> performlist=this.find(sql01);
....
667.                    TSysFlowlibmapform permform =
(TSysFlowlibmapform)performlist.get(0);
....
672.
      xml.append("<xid>"+permform.getFormid()+"</xid>");
....
675.                    xml.append("<gid>"+gid+"</gid>");
....
677.                    xml.append("<baseinfo>0</baseinfo>");
678.
      xml.append("<formid>"+permform.getFormid()+"</formid>");
679.
      xml.append("<formver>"+permform.getFormver()+"</formver>");
680.                    xml.append("<uid></uid>");
681.                    xml.append("<fid>"+gid+"</fid>");
682.                    xml.append("<zt></zt>");
683.                    xml.append("<sxid>"+sxid+"</sxid>");
684.                    xml.append("<ctype>1</ctype>");
685.                    xml.append("<templateid></templateid>");
686.                    xml.append("<templateName></templateName>");
687.                    xml.append("<bz></bz>");
688.                    xml.append("<cclid></cclid>");
689.                    xml.append("<fname></fname>");
690.                    xml.append("<orinum></orinum>");
691.                    xml.append("<copynum></copynum>");
692.                    xml.append("<pid></pid>");
693.                    xml.append("<clbh></clbh>");
....
711.                    xml.append("</form>\n");
....
796.              xml.append("<length>"+i+"</length>");
797.              xml.append("</formlist>");
798.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSysFlowlibmapform.java

方法 public String getFormid() {

```
....
31.         return formid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法	public String getFormInfoXml(String sxid, String groupid) {

```
....
42.         String xml = this.matterDao.getFormInfoXml(sxid, groupid);
43.         return xml;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String form(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
312.                     xml =
matterService.getFormInfoXml(sxid,groupid);
....
321.              out.print(xml);
```

Stored XSS\路径 3376:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3376
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	51	341
对象	list	print

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
445.              List list = this.find(sql02);
446.              if(list != null && list.size() > 0){
447.                    TXmlClob clob = (TXmlClob)list.get(0);
448.                    if(clob.getFileid() != null &&
!clob.getFileid().equals("")){
449.                          html = "#fileid:"+clob.getFileid();
....
454.              return html;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TXmlClob.java

方法 public String getFileid() {

```
....
81.         return fileid;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
384.                    xml.append(getFormInfoHtmlData(null, null,
insform
....
386.                    xml.append("]]></formhtmldata>");
387.                    xml.append("</form>\n");
....
434.              xml.append("<length>"+i+"</length>");
435.              xml.append("</formlist>");
436.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String bsid) throws Exception{

```
....
51.         String xml = this.matterDao.getFormInfoHtmlXml(bsid);
52.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
336.                    xml = matterService.getFormInfoHtmlXml(bsid);
....
341.              out.print(xml);
```

Stored XSS\路径 3377:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3377
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	51	362
对象	list	print

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java
方法	public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
445.              List list = this.find(sql02);
446.              if(list != null && list.size() > 0){
447.                    TXmlClob clob = (TXmlClob)list.get(0);
448.                    if(clob.getFileid() != null &&
!clob.getFileid().equals("")){
449.                          html = "#fileid:"+clob.getFileid();
....
454.              return html;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TXmlClob.java
方法	public String getFileid() {

```
....
81.         return fileid;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java
方法	public String getFormInfoHtmlData(String sxid,String formid,String formver,String groupid) {

```
....
55.         String xml =
this.matterDao.getFormInfoHtmlData(sxid,formid,formver,groupid);
56.         return xml;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String wssbForm(String sxid,String formid,String formver,String groupid,String bsid, HttpServletRequest request,

```
....
354.                    xml =
matterService.getFormInfoHtmlData(sxid,formid,formver,groupid);
....
362.              out.print(xml);
```

Stored XSS\路径 3378:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3378
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	51	953
对象	list	print

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java
方法	protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public List findBySql(String querySql) throws Exception {

```
....
948.              return this.find(querySql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getPostInfo(String sxid, CmsUser user) throws Exception{

```
....
93.          List infoList = this.matterDao.findBySql("from
TWebhallPermissionitemPost t where t.sxid='"+sxid+"' and
t.changetype<>'D' ");
....
95.          if(infoList.size()>0) post =
(TWebhallPermissionitemPost)infoList.get(0);
....
98.
      fb.append("<spsljg_dh>"+(post.getSpsljg_dh()==null?"":post.getSpsl
jg_dh())+"</spsljg_dh>");
99.
      fb.append("<spsljg_dw>"+(post.getSpsljg_dw()==null?"":post.getSpsl
jg_dw())+"</spsljg_dw>");
100.
      fb.append("<spsljg_dz>"+(post.getSpsljg_dz()==null?"":post.getSpsl
jg_dz())+"</spsljg_dz>");
101.
      fb.append("<spsljg_yb>"+(post.getSpsljg_yb()==null?"":post.getSpsl
jg_yb())+"</spsljg_yb>");
102.
      fb.append("<spsljg_id>"+(post.getId()==null?"":post.getId())+"</sp
sljg_id>");
103.               fb.append("<app_xm>"+user.getRealname()+"</app_xm>");
104.               fb.append("<app_dw>"+user.getIntro()+"</app_dw>");
....
128.                     fb.append("<app_dz></app_dz>");
129.                     fb.append("<app_yb></app_yb>");
....
131.               fb.append("<app_dh>"+user.getPhone()+"</app_dh>");
132.               fb.append("<app_sj>"+user.getMobile()+"</app_sj>");
133.               fb.append("</root>");
134.               return fb.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPermissionitemPost.java

方法 public String getSpsljg_dh() {

```
....
62.          return spsljg_dh;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostInfo(String sxid, HttpServletRequest request,

```
....
953.              out.print(matterService.getPostInfo(sxid,user));
```

Stored XSS\路径 3379:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3379
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	51	968
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(String hql, Object... values) {

```
....
51.         return createQuery(hql, values).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public List findBySql(String querySql) throws Exception {

```
....
948.              return this.find(querySql);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getPostInsInfo(String bsnum) throws Exception{

```
....
139.              List infoList = this.matterDao.findBySql("from
TWebhallPost t where t.id='"+bsnum+"' and t.changetype<>'D' ");
....
141.              if(infoList.size()>0) {
142.                    post = (TWebhallPost)infoList.get(0);
143.                    return post.getMaterial();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPost.java

方法 public String getMaterial() {

```
....
40.         return material;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getPostinsInfo(String bsnum, HttpServletRequest request,

```
....
968.             out.print(matterService.getPostInsInfo(bsnum));
```

Stored XSS\路径 3380:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3380
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	101	341
对象	list	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateSimpleDao.java

方法 protected List find(Finder finder) {

```
....
101.             List list = query.list();
102.             return list;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormHtmlXml(String userid){

```
....
321.                    List<TWebHallUserInforMation> webhalluserlist =
this.find("from TWebHallUserInforMation where useruid='"+userid+"'");
....
331.                            TWebHallUserInforMation webhalluser =
webhalluserlist.get(0);
332.                            webhalluser.setUser(null);
333.
      webhalluser.setYear(now.get(Calendar.YEAR)+"");
334.
      webhalluser.setMonth(now.get(Calendar.MONTH)+1+"");
335.
      webhalluser.setDay(now.get(Calendar.DAY_OF_MONTH)+"");
336.                            json = JSONObject.fromObject(webhalluser);
....
339.              return json.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/MatterDaoImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid){

```
....
135.              String userJson = getFormHtmlXml(userid);
....
137.              xml.append(userJson);
138.              xml.append("]]></userjson>");
....
248.              xml.append("<length>" + i + "</length>");
249.              xml.append("</formlist>");
....
251.              return xml.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/MatterServiceImpl.java

方法 public String getFormInfoHtmlXml(String sxid,String groupid,String userid) {

```
....
46.         String xml =
this.matterDao.getFormInfoHtmlXml(sxid,groupid,userid);
47.         return xml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String formHtml(String sxid,String groupid,String bsid, HttpServletRequest request,

```
....
333.                    xml =
matterService.getFormInfoHtmlXml(sxid,groupid,user.getId()+"");
....
341.              out.print(xml);
```

Stored XSS\路径 3381:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3381
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsTopicDaoImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
行	54	70
对象	list	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/CmsTopicDaoImpl.java

方法 public List<CmsTopic> getListByChannelIds(Integer[] channelIds) {

```
....
54.                     .setParameterList("ids", channelIds).list();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/CmsTopicMngImpl.java

方法 public List<CmsTopic> getListByChannel(Integer channelId) {

```
....
43.         list.addAll(dao.getListByChannelIds(c.getNodeIds()));
44.         return list;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/admin/main/CmsTopicAct.java

方法 public void topicsByChannel(Integer channelId, HttpServletResponse response)

```
....
163.                     List<CmsTopic> list =
manager.getListByChannel(channelId);
....
165.                     for (CmsTopic t : list) {
....
167.                         o.put("id", t.getId());
168.                         o.put("name", t.getName());
169.                         arr.put(o);
....
172.             ResponseUtils.renderJson(response, arr.toString());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
方法	public static void renderJson(HttpServletResponse response, String text) {

```
....
40.   public static void renderJson(HttpServletResponse response, String
text) {
41.         render(response, "application/json;charset=UTF-8", text);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/web/ResponseUtils.java
方法	public static void render(HttpServletResponse response, String contentType,

```
....
64.               String text) {
....
70.               response.getWriter().write(text);
```

Stored XSS\路径 3382:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3382
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	18	491
对象	find	print

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TInsYwpzServiceImpl.java
方法	public TInsYwpz getYwpz(String ywbh, String type) throws Exception {

```
....
18.         return (TInsYwpz)super.find("from TInsYwpz t where
t.ywbh='"+ywbh+"' and t.type='"+type+"'").get(0);
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java
方法	public String getYwpzXml(String bsnum,String type){

```
....
83.                 ywpz=TInsYwpzService.getYwpz(bsnum, type);
....
90.          return ywpz.getDataXml();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TInsYwpz.java

方法 public String getDataXml() {

```
....
97.    return dataXml;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getSbpzXml(String bsnum,String type, HttpServletRequest request,

```
....
490.              sqpz_xml=wssbService.getYwpzXml(bsnum,type);
491.              out.print(sqpz_xml);
```

Stored XSS\路径 3383:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3383
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	15	524
对象	find	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/tSharePostImpl.java

方法 public TSharePost getTSharePost(String sxid) {

```
....
15.         List list=super.find("from TSharePost t where
t.sxid='"+sxid+"'");
16.         if(!list.isEmpty()){
17.               t=(TSharePost)list.get(0);
....
19.         return  t;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/WssbServiceImp.java

方法 public String getSharePost(String sxid){

```
....
97.         TSharePost t=tsharePostService.getTSharePost(sxid);
....
102.                    str.append("<sxid>"+t.getSxid()+"</sxid>");
103.
      str.append("<spsljg_dw>"+t.getSpsljg_dw()+"</spsljg_dw>");//单位名称
104.
      str.append("<spsljg_dz>"+t.getSpsljg_dz()+"</spsljg_dz>");//地址
105.
      str.append("<spsljg_yb>"+t.getSpsljg_yb()+"</spsljg_yb>");//邮编
106.
      str.append("<spsljg_dh>"+t.getSpsljg_dh()+"</spsljg_dh>");//电话
107.                    str.append("</sharePost>");
....
113.              return str.toString();
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TSharePost.java

方法 public String getSpsljg_dz() {

```
....
52.         return spsljg_dz;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
501.              sfzc_xml=wssbService.getSharePost(sxid);
....
522.              str.append(sfzc_xml);
523.              str.append("</bsnumPost>");
524.              out.print(str.toString());
```

Stored XSS\路径 3384:

严重程度： 高风险
结果状态： 等待确认
在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3384

结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java
行	118	119
对象	buf	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/Zipper.java

方法 private void zip(File srcFile, FilenameFilter filter, ZipEntry pentry,

```
....
118.                                while ((len = in.read(buf)) > 0) {
....
102.                           zip(f, filter, entry, prefix);
....
119.                                     zipOut.write(buf, 0, len);
```

Stored XSS\路径 3385:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3385
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/SmartUpload.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/SmartUpload.java
行	319	321
对象	abyte0	write

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/util/jspsmart/upload/SmartUpload.java

方法 public void downloadFile(String s, String s1, String s2, int i)

```
....
319.              int j = fileinputstream.read(abyte0, 0, i);
....
321.              m_response.getOutputStream().write(abyte0, 0, j);
```

Stored XSS\路径 3386:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3386
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	57	524
对象	get	print

代码片断	
文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java
方法	protected T get(ID id, boolean lock) {

```
....
57.                 entity = (T) getSession().get(getEntityClass(), id,
....
62.         return entity;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallPostServiceImpl.java
方法	public TWebhallPost getPost(String bsnum){

```
....
34.         t=(TWebhallPost)dao.get(TWebhallPost.class, bsnum);
35.         return t;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
508.                    TWebhallPost t=postService.getPost(bsnum);
....
513.
      str.append("<material>"+t.getMaterial()+"</material>");
514.
      str.append("<posttype>"+t.getPosttype()+"</posttype>");//1为材料
2为证书 3为双程
....
522.              str.append(sfzc_xml);
523.              str.append("</bsnumPost>");
524.              out.print(str.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPost.java

方法 public String getPosttype() {

```
....
64.         return posttype;
```

Stored XSS\路径 3387:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3387
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	60	524
对象	get	print

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/hibernate3/HibernateBaseDao.java

方法 protected T get(ID id, boolean lock) {

```
....
60.               entity = (T) getSession().get(getEntityClass(), id);
....
62.         return entity;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallPostServiceImpl.java

方法	public TWebhallPost getPost(String bsnum){

```
....
34.         t=(TWebhallPost)dao.get(TWebhallPost.class, bsnum);
35.         return t;
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
方法	public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
508.                    TWebhallPost t=postService.getPost(bsnum);
....
513.
      str.append("<material>"+t.getMaterial()+"</material>");
514.
      str.append("<posttype>"+t.getPosttype()+"</posttype>");//1为材料
2为证书 3为双程
....
522.              str.append(sfzc_xml);
523.              str.append("</bsnumPost>");
524.              out.print(str.toString());
```

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPost.java
方法	public String getPosttype() {

```
....
64.         return posttype;
```

Stored XSS\路径 3388:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=3388
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java
行	43	524
对象	get	print

代码片断

文件名	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/dao/main/impl/TWebhallPostDAOImpl.java

方法 public Object get(Class clazz, Serializable id) {

```
....
43.       return getSession().get(clazz, id);
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/manager/main/impl/TWebhallPostServiceImpl.java

方法 public TWebhallPost getPost(String bsnum){

```
....
34.          t=(TWebhallPost)dao.get(TWebhallPost.class, bsnum);
35.          return t;
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/action/front/WssbAct.java

方法 public String getYzsd(String sxid,String bsnum, HttpServletRequest request,

```
....
508.                    TWebhallPost t=postService.getPost(bsnum);
....
513.
      str.append("<material>"+t.getMaterial()+"</material>");
514.
      str.append("<posttype>"+t.getPosttype()+"</posttype>");//1为材料
2为证书 3为双程
....
522.              str.append(sfzc_xml);
523.              str.append("</bsnumPost>");
524.              out.print(str.toString());
```

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/entity/main/TWebhallPost.java

方法 public String getPosttype() {

```
....
64.          return posttype;
```

Malicious Program

描述

Malicious Program\路径 18:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=18
结果评论	
被分配给	
状态	新的

来源	目的地

文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/WebYWLSHServiceImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/WebYWLSHServiceImpl.java
行	56	56
对象	executeMethod	executeMethod

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/WebYWLSHServiceImpl.java

方法 public String getywlsh(String sxbm) {

```
....
56.                 httpClient.executeMethod(postMethod);
```

Malicious Program\路径 19:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=19

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java
行	151	151
对象	execute	execute

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java

方法 private List<String> getContentList(HttpClient client,

```
....
151.                             String html = client.execute(httpget,
handler);
```

Malicious Program\路径 20:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=20

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java
行	195	195
对象	execute	execute

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/service/AcquisitionSvcImpl.java

方法 private Content saveContent(HttpClient client, CharsetHandler handler,

```
....
195.                            String html = client.execute(httpget,
handler);
```

Malicious Program\路径 21:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=21

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Content.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/Content.java
行	21	21
对象	openConnection	openConnection

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/Content.java

方法 public static String getUrlContent(String fileid) throws IOException {

```
....
21.                     .openConnection();
```

Malicious Program\路径 22:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=22

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/Shareinfopage.java	/WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/Shareinfopage.java
行	53	53
对象	openConnection	openConnection

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/cms/rest2/common/Shareinfopage.java

方法 public static boolean testUrl(){

```
....
53.          HttpURLConnection urlCon =
(HttpURLConnection)url.openConnection();
```

Malicious Program\路径 23:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=23

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageInfo.java	/WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageInfo.java
行	1003	1003
对象	openConnection	openConnection

代码片断

文件名 /WebHallCMSV3.0BAProject/src/com/jeecms/common/image/ImageInfo.java

方法 public static void main(String[] args) {

```
....
1003.                                        in = new
URL(name).openConnection().getInputStream();
```

Malicious Program\路径 24:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=24

结果评论

被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/util/SecureURL.java	/WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/util/SecureURL.java
行	68	68
对象	openConnection	openConnection

代码片断

文件名 /WebHallCMSV3.0BAProject/src/edu/yale/its/tp/cas/util/SecureURL.java

方法 public static String retrieve(String url) throws IOException {

```
....
68.             URLConnection uc = u.openConnection();
```

Client DOM XSS

描述

Client DOM XSS\路径 525:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=525
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js
行	85	85
对象	location	write

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js

方法

```
var FCKPanel=function(A){this.IsRTL=(FCKLang.Dir=='rtl');this.IsContextMenu=false;this._LockCounter=0;this._Window=A||window;var B;if (FCKBrowserInfo.IsIE){this._Popup=this._Window.createPopup();var C=this._Window.document;if (FCK_IS_CUSTOM_DOMAIN&&!FCKBrowserInfo.IsIE7){C.domain=FCK_ORIGINAL_DOMAIN;document.domain=FCK_ORIGINAL_DOMAIN;};B=this.Document=this._Popup.document;if (FCK_IS_CUSTOM_DOMAIN){B.domain=FCK_RUNTIME_DOMAIN;C.domain=FCK_RUNTIME_DOMAIN;document.domain=FCK_RUNTIME_DOMAIN;};FCK.IECleanup.AddItem(this,FCKPanel_Cleanup);}else{var D=this._IFrame=this._Window.document.createElement('iframe');FCKTools.ResetStyles(D);D.src='javascript:void(0)';D.allowTransparency=true;D.frameBorder='0';D.scrolling='no';D.style.width=D.style.height='0px';FCKDomTools.SetElementStyles(D,{position:'absolute',zIndex:FCKConfig.FloatingPanelsZIndex});this._Window.document.body.appendChild(D);var E=D.contentWindow;B=this.Document=E.document;var F='';if (FCKBrowserInfo.IsSafari) F='<base href="'+window.document.location+'">';B.open();B.write('<html><head>'+F+'<\/head><body style="margin:0px;padding:0px;"><\/body><\/html>');B.close();if(FCKBrowserInfo.IsAIR) FCKAdobeAIR.Panel_Contructor(B,window.document.location);FCKTools.AddEventListenerEx(E,'focus',FCKPanel_Window_OnFocus,this);FCKTools.AddEventListenerEx(E,'blur',FCKPanel_Window_OnBlur,this);};B.dir=FCKLang.Dir;FCKTools.AddEventListener(B,'contextmenu',FCKTools.CancelEvent);this.MainNode=B.body.appendChild(B.createElement('DIV'));this.MainNode.style.cssFloat=this.IsRTL?'right':'left';};FCKPanel.prototype.AppendStyleSheet=function(A){FCKTools.AppendStyleSheet(this.Document,A);};FCKPanel.prototype.Preload=function(x,y,A){if (this._Popup) this._Popup.show(x,y,0,0,A);};FCKPanel.prototype.ResizeForSubpanel=function(A,B,C){if (!FCKBrowserInfo.IsIE7) return false;if (!this._Popup.isOpen){this.Subpanel=null;return false;};if (B==0&&C==0){if (this.Subpanel!==A) return false;this.Subpanel=null;this.IncreasedX=0;}else{this.Subpanel=A;if ((this.IncreasedX>=B)&&(this.IncreasedY>=C)) return false;this.IncreasedX=Math.max(this.IncreasedX,B);this.IncreasedY=Math.max(this.IncreasedY,C);};var x=this.ShowRect.x;var w=this.IncreasedX;if (this.IsRTL) x=x-w;var D=this.ShowRect.w+w;var E=Math.max(this.ShowRect.h,this.IncreasedY);if (this.ParentPanel) this.ParentPanel.ResizeForSubpanel(this,D,E);this._Popup.show(x,this.ShowRect.y,D,E,this.RelativeElement);return this.IsRTL;};FCKPanel.prototype.Show=function(x,y,A,B,C){var D;var E=this.MainNode;if (this._Popup){this._Popup.show(x,y,0,0,A);FCKDomTools.SetElementStyles(E,{B:B?B+'px':'',C:C?C+'px':''});D=E.offsetWidth;if (FCKBrowserInfo.IsIE7){if (this.ParentPanel&&this.ParentPanel.ResizeForSubpanel(this,D,E.offsetHeight)){FCKTools.RunFunction(this.Show,this,[x,y,A]);return;}};if (this.IsRTL){if (this.IsContextMenu) x=x-D+1;else if (A) x=(x*-1)+A.offsetWidth-D;};if (FCKBrowserInfo.IsIE7){this.ShowRect={x:x,y:y,w:D,h:E.offsetHeight};this.IncreasedX=0;this.IncreasedY=0;this.RelativeElement=A;};this._Popup.show(x,y,D,E.offsetHeight,A);if (this.OnHide){if (this._Timer) CheckPopupOnHide.call(this,true);this._Timer=FCKTools.SetInterval(CheckPopupOnHide,100,this);}}else{if (typeof(FCK.ToolbarSet.CurrentInstance.FocusManager)!='undefined') FCK.ToolbarSet.CurrentInstance.FocusManager.Lock();if (this.ParentPanel){this.ParentPanel.Lock();FCKPanel_Window_OnBlur(null,this.ParentPanel);};if (FCKBrowserInfo.IsGecko&&FCKBrowserInfo.IsMac){this._IFrame.scrolling='';FCKTools.RunFunction(function(){ this._IFrame.scrolling='no';},this);};if
```

```
....
85.  var
FCKPanel=function(A){this.IsRTL=(FCKLang.Dir=='rtl');this.IsContextMenu=
false;this._LockCounter=0;this._Window=A||window;var B;if
(FCKBrowserInfo.IsIE){this._Popup=this._Window.createPopup();var
C=this._Window.document;if
(FCK_IS_CUSTOM_DOMAIN&&!FCKBrowserInfo.IsIE7){C.domain=FCK_ORIGINAL_DOMA
IN;document.domain=FCK_ORIGINAL_DOMAIN;};B=this.Document=this._Popup.doc
ument;if
(FCK_IS_CUSTOM_DOMAIN){B.domain=FCK_RUNTIME_DOMAIN;C.domain=FCK_RUNTIME_
DOMAIN;document.domain=FCK_RUNTIME_DOMAIN;};FCK.IECleanup.AddItem(this,F
CKPanel_Cleanup);}else{var
D=this._IFrame=this._Window.document.createElement('iframe');FCKTools.Re
setStyles(D);D.src='javascript:void(0)';D.allowTransparency=true;D.frame
Border='0';D.scrolling='no';D.style.width=D.style.height='0px';FCKDomToo
ls.SetElementStyles(D,{position:'absolute',zIndex:FCKConfig.FloatingPane
lsZIndex});this._Window.document.body.appendChild(D);var
E=D.contentWindow;B=this.Document=E.document;var F='';if
(FCKBrowserInfo.IsSafari) F='<base
href="'+window.document.location+'">';B.open();B.write('<html><head>'+F+
'<\/head><body
style="margin:0px;padding:0px;"><\/body><\/html>');B.close();if(FCKBrows
erInfo.IsAIR)
FCKAdobeAIR.Panel_Contructor(B,window.document.location);FCKTools.AddEve
ntListenerEx(E,'focus',FCKPanel_Window_OnFocus,this);FCKTools.AddEventLi
stenerEx(E,'blur',FCKPanel_Window_OnBlur,this);};B.dir=FCKLang.Dir;FCKTo
ols.AddEventListener(B,'contextmenu',FCKTools.CancelEvent);this.MainNode
=B.body.appendChild(B.createElement('DIV'));this.MainNode.style.cssFloat
=this.IsRTL?'right':'left';};FCKPanel.prototype.AppendStyleSheet=functio
n(A){FCKTools.AppendStyleSheet(this.Document,A);};FCKPanel.prototype.Pre
load=function(x,y,A){if (this._Popup)
this._Popup.show(x,y,0,0,A);};FCKPanel.prototype.ResizeForSubpanel=funct
ion(A,B,C){if (!FCKBrowserInfo.IsIE7) return false;if
(!this._Popup.isOpen){this.Subpanel=null;return false;};if
(B==0&&C==0){if (this.Subpanel!==A) return
false;this.Subpanel=null;this.IncreasedX=0;}else{this.Subpanel=A;if
((this.IncreasedX>=B)&&(this.IncreasedY>=C)) return
false;this.IncreasedX=Math.max(this.IncreasedX,B);this.IncreasedY=Math.m
ax(this.IncreasedY,C);};var x=this.ShowRect.x;var w=this.IncreasedX;if
(this.IsRTL) x=x-w;var D=this.ShowRect.w+w;var
E=Math.max(this.ShowRect.h,this.IncreasedY);if (this.ParentPanel)
this.ParentPanel.ResizeForSubpanel(this,D,E);this._Popup.show(x,this.Sho
wRect.y,D,E,this.RelativeElement);return
this.IsRTL;};FCKPanel.prototype.Show=function(x,y,A,B,C){var D;var
E=this.MainNode;if
(this._Popup){this._Popup.show(x,y,0,0,A);FCKDomTools.SetElementStyles(E
,{B:B?B+'px':'',C:C?C+'px':''});D=E.offsetWidth;if
(FCKBrowserInfo.IsIE7){if
(this.ParentPanel&&this.ParentPanel.ResizeForSubpanel(this,D,E.offsetHei
ght)){FCKTools.RunFunction(this.Show,this,[x,y,A]);return;}};if
(this.IsRTL){if (this.IsContextMenu) x=x-D+1;else if (A) x=(x*-
1)+A.offsetWidth-D;};if
(FCKBrowserInfo.IsIE7){this.ShowRect={x:x,y:y,w:D,h:E.offsetHeight};this
.IncreasedX=0;this.IncreasedY=0;this.RelativeElement=A;};this._Popup.sho
w(x,y,D,E.offsetHeight,A);if (this.OnHide){if (this._Timer)
CheckPopupOnHide.call(this,true);this._Timer=FCKTools.SetInterval(CheckP
opupOnHide,100,this);}}else{if
(typeof(FCK.ToolbarSet.CurrentInstance.FocusManager)!='undefined')
FCK.ToolbarSet.CurrentInstance.FocusManager.Lock();if
(this.ParentPanel){this.ParentPanel.Lock();FCKPanel_Window_OnBlur(null,t
his.ParentPanel);};if
(FCKBrowserInfo.IsGecko&&FCKBrowserInfo.IsMac){this._IFrame.scrolling=''
;FCKTools.RunFunction(function(){
this._IFrame.scrolling='no';},this);};if
(FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._OpenedPan
el&&FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._Opened
Panel!=this)
FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._OpenedPane
l.Hide(false,true);FCKDomTools.SetElementStyles(E,{B:B?B+'px':'',C:C?C+'
px':''});D=E.offsetWidth;if (!B)    this._IFrame.width=1;if (!C)
```

Client DOM XSS\路径 526:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=526
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js
行	86	86
对象	location	write

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js

方法

```
var FCKPanel=function(A){this.IsRTL=(FCKLang.Dir=='rtl');this.IsContextMenu=false;this._LockCounter=0;this._Window=A||window;var B;if (FCKBrowserInfo.IsIE){this._Popup=this._Window.createPopup();var C=this._Window.document;if (FCK_IS_CUSTOM_DOMAIN&&!FCKBrowserInfo.IsIE7){C.domain=FCK_ORIGINAL_DOMAIN;document.domain=FCK_ORIGINAL_DOMAIN;};B=this.Document=this._Popup.document;if (FCK_IS_CUSTOM_DOMAIN){B.domain=FCK_RUNTIME_DOMAIN;C.domain=FCK_RUNTIME_DOMAIN;document.domain=FCK_RUNTIME_DOMAIN;};FCK.IECleanup.AddItem(this,FCKPanel_Cleanup);}else{var D=this._IFrame=this._Window.document.createElement('iframe');FCKTools.ResetStyles(D);D.src='javascript:void(0)';D.allowTransparency=true;D.frameBorder='0';D.scrolling='no';D.style.width=D.style.height='0px';FCKDomTools.SetElementStyles(D,{position:'absolute',zIndex:FCKConfig.FloatingPanelsZIndex});this._Window.document.body.appendChild(D);var E=D.contentWindow;B=this.Document=E.document;var F='';if (FCKBrowserInfo.IsSafari) F='<base href="'+window.document.location+'">';B.open();B.write('<html><head>'+F+'<\/head><body style="margin:0px;padding:0px;"><\/body><\/html>');B.close();if(FCKBrowserInfo.IsAIR) FCKAdobeAIR.Panel_Contructor(B,window.document.location);FCKTools.AddEventListenerEx(E,'focus',FCKPanel_Window_OnFocus,this);FCKTools.AddEventListenerEx(E,'blur',FCKPanel_Window_OnBlur,this);};B.dir=FCKLang.Dir;FCKTools.AddEventListener(B,'contextmenu',FCKTools.CancelEvent);this.MainNode=B.body.appendChild(B.createElement('DIV'));this.MainNode.style.cssFloat=this.IsRTL?'right':'left';};FCKPanel.prototype.AppendStyleSheet=function(A){FCKTools.AppendStyleSheet(this.Document,A);};FCKPanel.prototype.Preload=function(x,y,A){if (this._Popup) this._Popup.show(x,y,0,0,A);};FCKPanel.prototype.ResizeForSubpanel=function(A,B,C){if (!FCKBrowserInfo.IsIE7) return false;if (!this._Popup.isOpen){this.Subpanel=null;return false;};if (B==0&&C==0){if (this.Subpanel!==A) return false;this.Subpanel=null;this.IncreasedX=0;}else{this.Subpanel=A;if ((this.IncreasedX>=B)&&(this.IncreasedY>=C)) return false;this.IncreasedX=Math.max(this.IncreasedX,B);this.IncreasedY=Math.max(this.IncreasedY,C);};var x=this.ShowRect.x;var w=this.IncreasedX;if (this.IsRTL) x=x-w;var D=this.ShowRect.w+w;var E=Math.max(this.ShowRect.h,this.IncreasedY);if (this.ParentPanel) this.ParentPanel.ResizeForSubpanel(this,D,E);this._Popup.show(x,this.ShowRect.y,D,E,this.RelativeElement);return this.IsRTL;};FCKPanel.prototype.Show=function(x,y,A,B,C){var D;var E=this.MainNode;if (this._Popup){this._Popup.show(x,y,0,0,A);FCKDomTools.SetElementStyles(E,{B:B?B+'px':'',C:C?C+'px':''});D=E.offsetWidth;if (FCKBrowserInfo.IsIE7){if (this.ParentPanel&&this.ParentPanel.ResizeForSubpanel(this,D,E.offsetHeight)){FCKTools.RunFunction(this.Show,this,[x,y,A]);return;}};if (this.IsRTL){if (this.IsContextMenu) x=x-D+1;else if (A) x=(x*-1)+A.offsetWidth-D;};if (FCKBrowserInfo.IsIE7){this.ShowRect={x:x,y:y,w:D,h:E.offsetHeight};this.IncreasedX=0;this.IncreasedY=0;this.RelativeElement=A;};this._Popup.show(x,y,D,E.offsetHeight,A);if (this.OnHide){if (this._Timer) CheckPopupOnHide.call(this,true);this._Timer=FCKTools.SetInterval(CheckPopupOnHide,100,this);}}else{if (typeof(FCK.ToolbarSet.CurrentInstance.FocusManager)!='undefined') FCK.ToolbarSet.CurrentInstance.FocusManager.Lock();if (this.ParentPanel){this.ParentPanel.Lock();FCKPanel_Window_OnBlur(null,this.ParentPanel);};if (FCKBrowserInfo.IsGecko&&FCKBrowserInfo.IsMac){this._IFrame.scrolling='';FCKTools.RunFunction(function(){ this._IFrame.scrolling='no';},this);};if
```

```
....
86.  var
FCKPanel=function(A){this.IsRTL=(FCKLang.Dir=='rtl');this.IsContextMenu=
false;this._LockCounter=0;this._Window=A||window;var B;if
(FCKBrowserInfo.IsIE){this._Popup=this._Window.createPopup();var
C=this._Window.document;if
(FCK_IS_CUSTOM_DOMAIN&&!FCKBrowserInfo.IsIE7){C.domain=FCK_ORIGINAL_DOMA
IN;document.domain=FCK_ORIGINAL_DOMAIN;};B=this.Document=this._Popup.doc
ument;if
(FCK_IS_CUSTOM_DOMAIN){B.domain=FCK_RUNTIME_DOMAIN;C.domain=FCK_RUNTIME_
DOMAIN;document.domain=FCK_RUNTIME_DOMAIN;};FCK.IECleanup.AddItem(this,F
CKPanel_Cleanup);}else{var
D=this._IFrame=this._Window.document.createElement('iframe');FCKTools.Re
setStyles(D);D.src='javascript:void(0)';D.allowTransparency=true;D.frame
Border='0';D.scrolling='no';D.style.width=D.style.height='0px';FCKDomToo
ls.SetElementStyles(D,{position:'absolute',zIndex:FCKConfig.FloatingPane
lsZIndex});this._Window.document.body.appendChild(D);var
E=D.contentWindow;B=this.Document=E.document;var F='';if
(FCKBrowserInfo.IsSafari) F='<base
href="'+window.document.location+'">';B.open();B.write('<html><head>'+F+
'<\/head><body
style="margin:0px;padding:0px;"><\/body><\/html>');B.close();if(FCKBrows
erInfo.IsAIR)
FCKAdobeAIR.Panel_Contructor(B,window.document.location);FCKTools.AddEve
ntListenerEx(E,'focus',FCKPanel_Window_OnFocus,this);FCKTools.AddEventLi
stenerEx(E,'blur',FCKPanel_Window_OnBlur,this);};B.dir=FCKLang.Dir;FCKTo
ols.AddEventListener(B,'contextmenu',FCKTools.CancelEvent);this.MainNode
=B.body.appendChild(B.createElement('DIV'));this.MainNode.style.cssFloat
=this.IsRTL?'right':'left';};FCKPanel.prototype.AppendStyleSheet=functio
n(A){FCKTools.AppendStyleSheet(this.Document,A);};FCKPanel.prototype.Pre
load=function(x,y,A){if (this._Popup)
this._Popup.show(x,y,0,0,A);};FCKPanel.prototype.ResizeForSubpanel=funct
ion(A,B,C){if (!FCKBrowserInfo.IsIE7) return false;if
(!this._Popup.isOpen){this.Subpanel=null;return false;};if
(B==0&&C==0){if (this.Subpanel!==A) return
false;this.Subpanel=null;this.IncreasedX=0;}else{this.Subpanel=A;if
((this.IncreasedX>=B)&&(this.IncreasedY>=C)) return
false;this.IncreasedX=Math.max(this.IncreasedX,B);this.IncreasedY=Math.m
ax(this.IncreasedY,C);};var x=this.ShowRect.x;var w=this.IncreasedX;if
(this.IsRTL) x=x-w;var D=this.ShowRect.w+w;var
E=Math.max(this.ShowRect.h,this.IncreasedY);if (this.ParentPanel)
this.ParentPanel.ResizeForSubpanel(this,D,E);this._Popup.show(x,this.Sho
wRect.y,D,E,this.RelativeElement);return
this.IsRTL;};FCKPanel.prototype.Show=function(x,y,A,B,C){var D;var
E=this.MainNode;if
(this._Popup){this._Popup.show(x,y,0,0,A);FCKDomTools.SetElementStyles(E
,{B:B?B+'px':'',C:C?C+'px':''});D=E.offsetWidth;if
(FCKBrowserInfo.IsIE7){if
(this.ParentPanel&&this.ParentPanel.ResizeForSubpanel(this,D,E.offsetHei
ght)){FCKTools.RunFunction(this.Show,this,[x,y,A]);return;}};if
(this.IsRTL){if (this.IsContextMenu) x=x-D+1;else if (A) x=(x*-
1)+A.offsetWidth-D;};if
(FCKBrowserInfo.IsIE7){this.ShowRect={x:x,y:y,w:D,h:E.offsetHeight};this
.IncreasedX=0;this.IncreasedY=0;this.RelativeElement=A;};this._Popup.sho
w(x,y,D,E.offsetHeight,A);if (this.OnHide){if (this._Timer)
CheckPopupOnHide.call(this,true);this._Timer=FCKTools.SetInterval(CheckP
opupOnHide,100,this);}}else{if
(typeof(FCK.ToolbarSet.CurrentInstance.FocusManager)!='undefined')
FCK.ToolbarSet.CurrentInstance.FocusManager.Lock();if
(this.ParentPanel){this.ParentPanel.Lock();FCKPanel_Window_OnBlur(null,t
his.ParentPanel);};if
(FCKBrowserInfo.IsGecko&&FCKBrowserInfo.IsMac){this._IFrame.scrolling=''
;FCKTools.RunFunction(function(){
this._IFrame.scrolling='no';},this);};if
(FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._OpenedPan
el&&FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._Opened
Panel!=this)
FCK.ToolbarSet.CurrentInstance.GetInstanceObject('FCKPanel')._OpenedPane
l.Hide(false,true);FCKDomTools.SetElementStyles(E,{B:B?B+'px':'',C:C?C+'
px':''});D=E.offsetWidth;if (!B)    this._IFrame.width=1;if (!C)
```

Client DOM XSS\路径 527:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=527
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js
行	99	99
对象	location	write

代码片断	
文件名	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_gecko.js

方法

```
function FCKToolbarSet_Create(A){var B;var C=A||FCKConfig.ToolbarLocation;switch (C){case 'In':document.getElementById('xToolbarRow').style.display='';B=new FCKToolbarSet(document);break;case 'None':B=new FCKToolbarSet(document);break;default:FCK.Events.AttachEvent('OnBlur',FCK_OnBlur);FCK.Events.AttachEvent('OnFocus',FCK_OnFocus);var D;var E=C.match(/^Out:(.+)\((\w+)\)$/);if (E){if (FCKBrowserInfo.IsAIR) FCKAdobeAIR.ToolbarSet_GetOutElement(window,E);else D=eval('parent.'+E[1]).document.getElementById(E[2]);}else{E=C.match(/^Out:(\w+)$/);if (E) D=parent.document.getElementById(E[1]);};if (!D){alert('Invalid value for "ToolbarLocation"');return arguments.callee('In');};B=D.__FCKToolbarSet;if (B) break;var F=FCKTools.GetElementDocument(D).createElement('iframe');F.src='javascript:void(0)';F.frameBorder=0;F.width='100%';F.height='10';D.appendChild(F);F.unselectable='on';var G=F.contentWindow.document;var H='';if (FCKBrowserInfo.IsSafari) H='<base href="'+window.document.location+'">';G.open();G.write('<html><head>'+H+'<script type="text/javascript"> var adjust = function() { window.frameElement.height = document.body.scrollHeight ; }; window.onresize = window.onload = function(){var timer = null;var lastHeight = -1;var lastChange = 0;var poller = function(){var currentHeight = document.body.scrollHeight || 0;var currentTime = (new Date()).getTime();if (currentHeight != lastHeight){lastChange = currentTime;adjust();lastHeight = document.body.scrollHeight;}if (lastChange < currentTime - 1000) clearInterval(timer);};timer = setInterval(poller, 100);}</script></head><body style="overflow: hidden">'+document.getElementById('xToolbarSpace').innerHTML+'</body></html>');G.close();if(FCKBrowserInfo.IsAIR) FCKAdobeAIR.ToolbarSet_InitOutFrame(G);FCKTools.AddEventListener(G,'contextmenu',FCKTools.CancelEvent);FCKTools.AppendStyleSheet(G,FCKConfig.SkinEditorCSS);B=D.__FCKToolbarSet=new FCKToolbarSet(G);B._IFrame=F;if (FCK.IECleanup) FCK.IECleanup.AddItem(D,FCKToolbarSet_Target_Cleanup);};B.CurrentInstance=FCK;if (!B.ToolbarItems) B.ToolbarItems=FCKToolbarItems;FCK.AttachToOnSelectionChange(B.RefreshItemsState);return B;};function FCK_OnBlur(A){var B=A.ToolbarSet;if (B.CurrentInstance==A) B.Disable();};function FCK_OnFocus(A){var B=A.ToolbarSet;var C=A||FCK;B.CurrentInstance.FocusManager.RemoveWindow(B._IFrame.contentWindow);B.CurrentInstance=C;C.FocusManager.AddWindow(B._IFrame.contentWindow,true);B.Enable();};function FCKToolbarSet_Cleanup(){this._TargetElement=null;this._IFrame=null;};function FCKToolbarSet_Target_Cleanup(){this.__FCKToolbarSet=null;};var FCKToolbarSet=function(A){this._Document=A;this._TargetElement=A.getElementById('xToolbar');var B=A.getElementById('xExpandHandle');var C=A.getElementById('xCollapseHandle');B.title=FCKLang.ToolbarExpand;FCKTools.AddEventListener(B,'click',FCKToolbarSet_Expand_OnClick);C.title=FCKLang.ToolbarCollapse;FCKTools.AddEventListener(C,'click',FCKToolbarSet_Collapse_OnClick);if (!FCKConfig.ToolbarCanCollapse||FCKConfig.ToolbarStartExpanded) this.Expand();else this.Collapse();C.style.display=FCKConfig.ToolbarCanCollapse?'':'none';if (FCKConfig.ToolbarCanCollapse) C.style.display='';else A.getElementById('xTBLeftBorder').style.display='';this.Toolbars=[];this.IsLoaded=false;if (FCK.IECleanup) FCK.IECleanup.AddItem(this,FCKToolbarSet_Cleanup);};function FCKToolbarSet_Expand_OnClick(){FCK.ToolbarSet.Expand();};function FCKToolbarSet_Collapse_OnClick(){FCK.ToolbarSet.Collapse();};FCKToolbarSet.prototype.Expand=function(){this._ChangeVisibility(false);};FCKToolbarSet.prototype.Collapse=function(){this._ChangeVisibility(true);};FCKToolbarSet.prototype._ChangeVisibility=function(A){this._Document.getElementById('xCollapsed').styl
```

```
....
99.  function FCKToolbarSet_Create(A){var B;var
C=A||FCKConfig.ToolbarLocation;switch (C){case
'In':document.getElementById('xToolbarRow').style.display='';B=new
FCKToolbarSet(document);break;case 'None':B=new
FCKToolbarSet(document);break;default:FCK.Events.AttachEvent('OnBlur',FC
K_OnBlur);FCK.Events.AttachEvent('OnFocus',FCK_OnFocus);var D;var
E=C.match(/^Out:(.+)\((\w+)\)$/);if (E){if (FCKBrowserInfo.IsAIR)
FCKAdobeAIR.ToolbarSet_GetOutElement(window,E);else
D=eval('parent.'+E[1]).document.getElementById(E[2]);}else{E=C.match(/^O
ut:(\w+)$/);if (E) D=parent.document.getElementById(E[1]);};if
(!D){alert('Invalid value for "ToolbarLocation"');return
arguments.callee('In');};B=D.__FCKToolbarSet;if (B) break;var
F=FCKTools.GetElementDocument(D).createElement('iframe');F.src='javascri
pt:void(0)';F.frameBorder=0;F.width='100%';F.height='10';D.appendChild(F
);F.unselectable='on';var G=F.contentWindow.document;var H='';if
(FCKBrowserInfo.IsSafari) H='<base
href="'+window.document.location+'">';G.open();G.write('<html><head>'+H+
'<script type="text/javascript"> var adjust = function() {
window.frameElement.height = document.body.scrollHeight ; };
window.onresize = window.onload = function(){var timer = null;var
lastHeight = -1;var lastChange = 0;var poller = function(){var
currentHeight = document.body.scrollHeight || 0;var currentTime = (new
Date()).getTime();if (currentHeight != lastHeight){lastChange =
currentTime;adjust();lastHeight = document.body.scrollHeight;}if
(lastChange < currentTime - 1000) clearInterval(timer);};timer =
setInterval(poller, 100);}</script></head><body style="overflow:
hidden">'+document.getElementById('xToolbarSpace').innerHTML+'</body></h
tml>');G.close();if(FCKBrowserInfo.IsAIR)
FCKAdobeAIR.ToolbarSet_InitOutFrame(G);FCKTools.AddEventListener(G,'cont
extmenu',FCKTools.CancelEvent);FCKTools.AppendStyleSheet(G,FCKConfig.Ski
nEditorCSS);B=D.__FCKToolbarSet=new FCKToolbarSet(G);B._IFrame=F;if
(FCK.IECleanup)
FCK.IECleanup.AddItem(D,FCKToolbarSet_Target_Cleanup);};B.CurrentInstanc
e=FCK;if (!B.ToolbarItems)
B.ToolbarItems=FCKToolbarItems;FCK.AttachToOnSelectionChange(B.RefreshIt
emsState);return B;};function FCK_OnBlur(A){var B=A.ToolbarSet;if
(B.CurrentInstance==A) B.Disable();};function FCK_OnFocus(A){var
B=A.ToolbarSet;var
C=A||FCK;B.CurrentInstance.FocusManager.RemoveWindow(B._IFrame.contentWi
ndow);B.CurrentInstance=C;C.FocusManager.AddWindow(B._IFrame.contentWind
ow,true);B.Enable();};function
FCKToolbarSet_Cleanup(){this._TargetElement=null;this._IFrame=null;};fun
ction FCKToolbarSet_Target_Cleanup(){this.__FCKToolbarSet=null;};var
FCKToolbarSet=function(A){this._Document=A;this._TargetElement=A.getElem
entById('xToolbar');var B=A.getElementById('xExpandHandle');var
C=A.getElementById('xCollapseHandle');B.title=FCKLang.ToolbarExpand;FCKT
ools.AddEventListener(B,'click',FCKToolbarSet_Expand_OnClick);C.title=FC
KLang.ToolbarCollapse;FCKTools.AddEventListener(C,'click',FCKToolbarSet_
Collapse_OnClick);if
(!FCKConfig.ToolbarCanCollapse||FCKConfig.ToolbarStartExpanded)
this.Expand();else
this.Collapse();C.style.display=FCKConfig.ToolbarCanCollapse?'':'none';i
f (FCKConfig.ToolbarCanCollapse) C.style.display='';else
A.getElementById('xTBLeftBorder').style.display='';this.Toolbars=[];this
.IsLoaded=false;if (FCK.IECleanup)
FCK.IECleanup.AddItem(this,FCKToolbarSet_Cleanup);};function
FCKToolbarSet_Expand_OnClick(){FCK.ToolbarSet.Expand();};function
FCKToolbarSet_Collapse_OnClick(){FCK.ToolbarSet.Collapse();};FCKToolbarS
et.prototype.Expand=function(){this._ChangeVisibility(false);};FCKToolba
rSet.prototype.Collapse=function(){this._ChangeVisibility(true);};FCKToo
lbarSet.prototype._ChangeVisibility=function(A){this._Document.getElemen
tById('xCollapsed').style.display=A?'':'none';this._Document.getElementB
yId('xExpanded').style.display=A?'none':'';if
(FCKBrowserInfo.IsGecko){FCKTools.RunFunction(window.onresize);}};FCKToo
lbarSet.prototype.Load=function(A){this.Name=A;this.Items=[];this.ItemsW
ysiwygOnly=[];this.ItemsContextSensitive=[];this._TargetElement.innerHTM
L='';var B=FCKConfig.ToolbarSets[A];if
(!B){alert(FCKLang.UnknownToolbarSet.replace(/%1/g,A));return;};this.Too
lbars=[];for (var x=0;x<B.length;x++){var C=B[x];if (!C) continue;var
```

Client DOM XSS\路径 528:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=528
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js
行	100	100
对象	location	write

代码片断	
文件名	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/fckeditor/editor/js/fckeditorcode_ie.js

方法

```
function FCKToolbarSet_Create(A){var B;var C=A||FCKConfig.ToolbarLocation;switch (C){case 'In':document.getElementById('xToolbarRow').style.display='';B=new FCKToolbarSet(document);break;case 'None':B=new FCKToolbarSet(document);break;default:FCK.Events.AttachEvent('OnBlur',FCK_OnBlur);FCK.Events.AttachEvent('OnFocus',FCK_OnFocus);var D;var E=C.match(/^Out:(.+)\((\w+)\)$/);if (E){if (FCKBrowserInfo.IsAIR) FCKAdobeAIR.ToolbarSet_GetOutElement(window,E);else D=eval('parent.'+E[1]).document.getElementById(E[2]);}else{E=C.match(/^Out:(\w+)$/);if (E) D=parent.document.getElementById(E[1]);};if (!D){alert('Invalid value for "ToolbarLocation"');return arguments.callee('In');};B=D.__FCKToolbarSet;if (B) break;var F=FCKTools.GetElementDocument(D).createElement('iframe');F.src='javascript:void(0)';F.frameBorder=0;F.width='100%';F.height='10';D.appendChild(F);F.unselectable='on';var G=F.contentWindow.document;var H='';if (FCKBrowserInfo.IsSafari) H='<base href="'+window.document.location+'">';G.open();G.write('<html><head>'+H+'<script type="text/javascript"> var adjust = function() { window.frameElement.height = document.body.scrollHeight ; }; window.onresize = window.onload = function(){var timer = null;var lastHeight = -1;var lastChange = 0;var poller = function(){var currentHeight = document.body.scrollHeight || 0;var currentTime = (new Date()).getTime();if (currentHeight != lastHeight){lastChange = currentTime;adjust();lastHeight = document.body.scrollHeight;}if (lastChange < currentTime - 1000) clearInterval(timer);};timer = setInterval(poller, 100);}</script></head><body style="overflow: hidden">'+document.getElementById('xToolbarSpace').innerHTML+'</body></html>');G.close();if(FCKBrowserInfo.IsAIR) FCKAdobeAIR.ToolbarSet_InitOutFrame(G);FCKTools.AddEventListener(G,'contextmenu',FCKTools.CancelEvent);FCKTools.AppendStyleSheet(G,FCKConfig.SkinEditorCSS);B=D.__FCKToolbarSet=new FCKToolbarSet(G);B._IFrame=F;if (FCK.IECleanup) FCK.IECleanup.AddItem(D,FCKToolbarSet_Target_Cleanup);};B.CurrentInstance=FCK;if (!B.ToolbarItems) B.ToolbarItems=FCKToolbarItems;FCK.AttachToOnSelectionChange(B.RefreshItemsState);return B;};function FCK_OnBlur(A){var B=A.ToolbarSet;if (B.CurrentInstance==A) B.Disable();};function FCK_OnFocus(A){var B=A.ToolbarSet;var C=A||FCK;B.CurrentInstance.FocusManager.RemoveWindow(B._IFrame.contentWindow);B.CurrentInstance=C;C.FocusManager.AddWindow(B._IFrame.contentWindow,true);B.Enable();};function FCKToolbarSet_Cleanup(){this._TargetElement=null;this._IFrame=null;};function FCKToolbarSet_Target_Cleanup(){this.__FCKToolbarSet=null;};var FCKToolbarSet=function(A){this._Document=A;this._TargetElement=A.getElementById('xToolbar');var B=A.getElementById('xExpandHandle');var C=A.getElementById('xCollapseHandle');B.title=FCKLang.ToolbarExpand;FCKTools.AddEventListener(B,'click',FCKToolbarSet_Expand_OnClick);C.title=FCKLang.ToolbarCollapse;FCKTools.AddEventListener(C,'click',FCKToolbarSet_Collapse_OnClick);if (!FCKConfig.ToolbarCanCollapse||FCKConfig.ToolbarStartExpanded) this.Expand();else this.Collapse();C.style.display=FCKConfig.ToolbarCanCollapse?'':'none';if (FCKConfig.ToolbarCanCollapse) C.style.display='';else A.getElementById('xTBLeftBorder').style.display='';this.Toolbars=[];this.IsLoaded=false;if (FCK.IECleanup) FCK.IECleanup.AddItem(this,FCKToolbarSet_Cleanup);};function FCKToolbarSet_Expand_OnClick(){FCK.ToolbarSet.Expand();};function FCKToolbarSet_Collapse_OnClick(){FCK.ToolbarSet.Collapse();};FCKToolbarSet.prototype.Expand=function(){this._ChangeVisibility(false);};FCKToolbarSet.prototype.Collapse=function(){this._ChangeVisibility(true);};FCKToolbarSet.prototype._ChangeVisibility=function(A){this._Document.getElementById('xCollapsed').styl
```

```
....
100.  function FCKToolbarSet_Create(A){var B;var
C=A||FCKConfig.ToolbarLocation;switch (C){case
'In':document.getElementById('xToolbarRow').style.display='';B=new
FCKToolbarSet(document);break;case 'None':B=new
FCKToolbarSet(document);break;default:FCK.Events.AttachEvent('OnBlur',FC
K_OnBlur);FCK.Events.AttachEvent('OnFocus',FCK_OnFocus);var D;var
E=C.match(/^Out:(.+)\((\w+)\)$/);if (E){if (FCKBrowserInfo.IsAIR)
FCKAdobeAIR.ToolbarSet_GetOutElement(window,E);else
D=eval('parent.'+E[1]).document.getElementById(E[2]);}else{E=C.match(/^O
ut:(\w+)$/);if (E) D=parent.document.getElementById(E[1]);};if
(!D){alert('Invalid value for "ToolbarLocation"');return
arguments.callee('In');};B=D.__FCKToolbarSet;if (B) break;var
F=FCKTools.GetElementDocument(D).createElement('iframe');F.src='javascri
pt:void(0)';F.frameBorder=0;F.width='100%';F.height='10';D.appendChild(F
);F.unselectable='on';var G=F.contentWindow.document;var H='';if
(FCKBrowserInfo.IsSafari) H='<base
href="'+window.document.location+'">';G.open();G.write('<html><head>'+H+
'<script type="text/javascript"> var adjust = function() {
window.frameElement.height = document.body.scrollHeight ; };
window.onresize = window.onload = function(){var timer = null;var
lastHeight = -1;var lastChange = 0;var poller = function(){var
currentHeight = document.body.scrollHeight || 0;var currentTime = (new
Date()).getTime();if (currentHeight != lastHeight){lastChange =
currentTime;adjust();lastHeight = document.body.scrollHeight;}if
(lastChange < currentTime - 1000) clearInterval(timer);};timer =
setInterval(poller, 100);}</script></head><body style="overflow:
hidden">'+document.getElementById('xToolbarSpace').innerHTML+'</body></h
tml>');G.close();if(FCKBrowserInfo.IsAIR)
FCKAdobeAIR.ToolbarSet_InitOutFrame(G);FCKTools.AddEventListener(G,'cont
extmenu',FCKTools.CancelEvent);FCKTools.AppendStyleSheet(G,FCKConfig.Ski
nEditorCSS);B=D.__FCKToolbarSet=new FCKToolbarSet(G);B._IFrame=F;if
(FCK.IECleanup)
FCK.IECleanup.AddItem(D,FCKToolbarSet_Target_Cleanup);};B.CurrentInstanc
e=FCK;if (!B.ToolbarItems)
B.ToolbarItems=FCKToolbarItems;FCK.AttachToOnSelectionChange(B.RefreshIt
emsState);return B;};function FCK_OnBlur(A){var B=A.ToolbarSet;if
(B.CurrentInstance==A) B.Disable();};function FCK_OnFocus(A){var
B=A.ToolbarSet;var
C=A||FCK;B.CurrentInstance.FocusManager.RemoveWindow(B._IFrame.contentWi
ndow);B.CurrentInstance=C;C.FocusManager.AddWindow(B._IFrame.contentWind
ow,true);B.Enable();};function
FCKToolbarSet_Cleanup(){this._TargetElement=null;this._IFrame=null;};fun
ction FCKToolbarSet_Target_Cleanup(){this.__FCKToolbarSet=null;};var
FCKToolbarSet=function(A){this._Document=A;this._TargetElement=A.getElem
entById('xToolbar');var B=A.getElementById('xExpandHandle');var
C=A.getElementById('xCollapseHandle');B.title=FCKLang.ToolbarExpand;FCKT
ools.AddEventListener(B,'click',FCKToolbarSet_Expand_OnClick);C.title=FC
KLang.ToolbarCollapse;FCKTools.AddEventListener(C,'click',FCKToolbarSet_
Collapse_OnClick);if
(!FCKConfig.ToolbarCanCollapse||FCKConfig.ToolbarStartExpanded)
this.Expand();else
this.Collapse();C.style.display=FCKConfig.ToolbarCanCollapse?'':'none';i
f (FCKConfig.ToolbarCanCollapse) C.style.display='';else
A.getElementById('xTBLeftBorder').style.display='';this.Toolbars=[];this
.IsLoaded=false;if (FCK.IECleanup)
FCK.IECleanup.AddItem(this,FCKToolbarSet_Cleanup);};function
FCKToolbarSet_Expand_OnClick(){FCK.ToolbarSet.Expand();};function
FCKToolbarSet_Collapse_OnClick(){FCK.ToolbarSet.Collapse();};FCKToolbarS
et.prototype.Expand=function(){this._ChangeVisibility(false);};FCKToolba
rSet.prototype.Collapse=function(){this._ChangeVisibility(true);};FCKToo
lbarSet.prototype._ChangeVisibility=function(A){this._Document.getElemen
tById('xCollapsed').style.display=A?'':'none';this._Document.getElementB
yId('xExpanded').style.display=A?'none':'';if
(FCKBrowserInfo.IsGecko){FCKTools.RunFunction(window.onresize);}};FCKToo
lbarSet.prototype.Load=function(A){this.Name=A;this.Items=[];this.ItemsW
ysiwygOnly=[];this.ItemsContextSensitive=[];this._TargetElement.innerHTM
L='';var B=FCKConfig.ToolbarSets[A];if
(!B){alert(FCKLang.UnknownToolbarSet.replace(/%1/g,A));return;};this.Too
lbars=[];for (var x=0;x<B.length;x++){var C=B[x];if (!C) continue;var
```

Client DOM XSS\路径 529:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=529
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js	/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js
行	791	806
对象	protocol	append

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js

方法 $.post("/wssb/sbsubmit.jspx",param,function(data){

```
....
791.                    var
path=window.location.protocol+'//'+window.location.host+'/'+getPath();
....
795.                    "<td align=\"center\"><img
src=\""+path+"/images/ewm2.jpg\" width=\"75\" height=\"75\" /><br />\n"
+
....
792.                    tempStr+="\n" +
....
806.                    $('#sbweb_sbpz').append(tempStr);
```

Client DOM XSS\路径 530:

严重程度：	高风险
结果状态：	等待确认
在线结果：	http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=530
结果评论	
被分配给	
状态	新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js	/WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js
行	791	806
对象	host	append

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/r/cms/matterhtmlshow.js

方法 $.post("/wssb/sbsubmit.jspx",param,function(data){

```
....
791.                    var
path=window.location.protocol+'//'+window.location.host+'/'+getPath();
....
795.                    "<td align=\"center\"><img
src=\""+path+"/images/ewm2.jpg\" width=\"75\" height=\"75\" /><br />\n"
+
....
792.                    tempStr+="\n" +
....
806.                    $('#sbweb_sbpz').append(tempStr);
```

Client DOM XSS\路径 531:

严重程度： 高风险

结果状态： 等待确认

在线结果： http://WINDOWS-9HSCNS6/CxWebClient/ViewerMain.aspx?scanid=1027&projectid=1188&pathid=531

结果评论

被分配给

状态 新的

	来源	目的地
文件	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js	/WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js
行	822	832
对象	host	innerHTML

代码片断

文件名 /WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js

方法 var _bridge = function() {

```
....
822.        var allowScriptAccess =
_determineScriptAccess(window.location.host, _globalConfig);
....
832.        tmpDiv.innerHTML = '<object id="global-zeroclipboard-flash-
bridge" name="global-zeroclipboard-flash-bridge" ' + 'width="100%"
height="100%" ' + (oldIE ? 'classid="clsid:d27cdb6e-ae6d-11cf-96b8-
444553540000"' : 'type="application/x-shockwave-flash" data="' + swfUrl
+ '"') + ">" + (oldIE ? '<param name="movie" value="' + swfUrl + '"/>' :
"") + '<param name="allowScriptAccess" value="' + allowScriptAccess +
'"/>' + '<param name="allowNetworking" value="' + allowNetworking +
'"/>' + '<param name="menu" value="false"/>' + '<param name="wmode"
value="transparent"/>' + '<param name="flashvars" value="' + flashvars +
'"/>' + "</object>";
```

文件名 /WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js

方法 var _determineScriptAccess = function() {

```
....
351.    var _determineScriptAccess = function() {
....
376.      return function(currentDomain, configOptions) {
```

文件名 /WebHallCMSV3.0BAProject/WebRoot/thirdparty/ueditor/third-party/zeroclipboard/ZeroClipboard.js

方法 var swfDomain = _extractDomain(configOptions.swfPath);

```
....
376.      return function(currentDomain, configOptions) {
....
379.          swfDomain = currentDomain;
```

Privilege / Sandbox Issues

Category ID: 265 (Category) **Status:** Incomplete

Description

简要描述

这一类漏洞伴随着错误的执行沙盒环境，或任务分派处理不当，或特权的管理而出现。

可能的漏洞消除办法

非常仔细地管理权限的设置，操纵和处理特权。明确管理软件的信任区。

分配一个软件系统中实体的访问权限时，按照最小特权原则。

Relationships

Nature	Type	ID	Name	
ChildOf		264	Permissions, Privileges, and Access Controls	699
ParentOf		266	Incorrect Privilege Assignment	699
ParentOf		267	Privilege Defined With Unsafe Actions	699
ParentOf		268	Privilege Chaining	699
ParentOf		269	Improper Privilege Management	699
ParentOf		271	Privilege Dropping / Lowering Errors	699
ParentOf		274	Improper Handling of Insufficient Privileges	699
ParentOf		610	Externally Controlled Reference to a Resource in Another Sphere	699

ParentOf		648	Incorrect Use of Privileged APIs	**699**
PeerOf		250	Execution with Unnecessary Privileges	1000
PeerOf		619	Dangling Database Cursor ('Cursor Injection')	1000

Relationship Notes

这可以强烈地重叠授权错误。

研究空白

许多下述的概念需要更深层次的研究。大多数特权问题并非分类在如此低层次的细节和稀疏的术语中。某些类型的软件，如web浏览器和软件bug追踪器，为进一步研究提供了一组丰富的例子。操作系统已经足够成熟，以至于这些类型的漏洞已经很少见，但是更细微的模型，能力，或角色等特权可能会引入微妙的问题。

理论注释

一个沙箱可以被看作是一个明确定义的控制范围，在这里沙箱只定义了一组有限的行为，这个行为只能访问一组有限的资源。

有人可能会认为，任何特权问题都发生在沙箱环境之内。

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	适用于	Mapped Node Name
PLOVER			Privilege / sandbox errors

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Relationship Notes, Taxonomy Mappings, Theoretical Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description, Research Gaps, Theoretical Notes		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

BACK TO TOP

Privacy Violation

Weakness ID: 359 (Weakness Class) **Status:** Incomplete

描述

简要描述

对客户密码或社会安全号码（social security numbers）等私人信息处理不当可能损害用户的隐私，而且这往往也是非法的。

引入阶段

- 构架与设计阶段
- 实现阶段
- 操作阶段

适用平台

语言

所有

示例

示例1

下面的代码中包含了一条记录日志的语句，该语句通过存储到日志文件的方式来跟踪被保存到数据库中的记录内容。在所有储存的值中，只有getPassword()函数返回与帐户相关联的由用户提供的明文密码中。

(Bad Code)

Example Language: **C#**

```
pass = GetPassword();
...
dbmsLog.WriteLine(id + ":" + pass + ":" + type + ":" + tstamp);
```

上面例子中的代码中将明文密码记录到了filesystem中。虽然许多开发者都相信filesystem是数据存储的安全位置，但在涉及到隐私的时候，仍然不应过分信赖filesystem。

其它注释

在下列情况下会发生隐私受侵犯：1.用户的私人信息进入程序。2.数据被写入外部位置，如控制台、文件系统或网络中。

私人数据可以通过各种不同的方式进入到程序中：

- 通过密码或个人信息的形式直接从用户那里进入
- 通过访问数据库或应用程序储存的其它数据
- 从合作伙伴或其他第三方那里间接进入

有时数据虽然没有被标记为私人信息，但在不同的情况下，仍然可能包含有隐私信息。例如，通常学生证号不被视为隐私信息，因为学生证号中没有明确公开的信息可以映射到个别学生的个人信息。但是，如果学校以学生的社会安全号码SSN为基础而生成学生证号，那么这样的学生证号就应被视为隐私信息。

安全和隐私似乎经常在互相竞争。从安全角度来说，你应该对所有重要的行动进行记录，以便于日后对异常活动进行确定。但，一旦涉及到隐私数据，这种做法本身就可能成为安全隐患。虽然用来处理隐私数据中的很多方法都并不安全，但这些不安全方法中一个共同危险都在于信任了不该被信任的情况。程序员往往会对程序运行的环境很信任，因此认为可以将隐私信息存储在文件系统中、注册表中，或其他本地控制的资源中。但，即使对某些资源的访问是受限制的，这也并不保证拥有访问权限的个人是值得信赖的。

例如，2004年，美国在线的一名肆无忌惮的员工向一家经营境外赌博网站[23]的垃圾邮件制造者出售了约9200万份个人用户电子邮件地址。针对这种明目张胆的利用，收集和管理私人数据正变得越来越规范。根据其位置、业务类型及处理中的隐私数据性质，公司应该遵守一个或多个下面的联邦或州的规定：- Safe Harbor Privacy Framework [24] - Gramm-Leach Bliley Act (GLBA) [11] - Health Insurance Portability and Accountability Act (HIPAA) [16] - California SB-1386 [6]

关系

性质	类型	ID	名称	
ChildOf		200	Information Exposure	**1000**
ChildOf		254	Security Features	**699** **700**
ParentOf		202	Privacy Leak through Data Queries	**1000**

缺陷类别映射

映射分类	节点	适用于	映射节点名称
7 Pernicious Kingdoms			Privacy Violation

参考

J. Oates. "AOL man pleads guilty to selling 92m email addies". The Register. 2005. <http://www.theregister.co.uk/2005/02/07/aol_email_theft/>.

[REF-2] U.S. Department of Commerce. "Safe Harbor Privacy Framework". <http://www.export.gov/safeharbor/>.

[REF-3] Federal Trade Commission. "Financial Privacy: The Gramm-Leach Bliley Act (GLBA)". <http://www.ftc.gov/privacy/glbact/index.html>.

[REF-4] U.S. Department of Human Services. "Health Insurance Portability and Accountability Act (HIPAA)". <http://www.hhs.gov/ocr/hipaa/>.

[REF-5] Government of the State of California. "California SB-1386". 2002. <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	7 Pernicious Kingdoms		Externally Mined
修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Other Notes, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Other Notes, References		

BACK TO TOP

Failure to Preserve Web Page Structure ('Cross-site Scripting')

Weakness **Status:** Usable

ID: 79 (Weakness Base)

描述

简要描述

该软件没有对用户可控的输入数据进行充分验证、过滤、避免和/或Encode，就将其放在输出数据中，用于WEB页面服务于其他用户。

扩展描述

当下列情况发生时，出现跨站脚本（XSS）漏洞：

1. 非信任的数据进入Web应用程序中，这样的数据通常来自于Web请求。

2. Web应用程序动态生成一个包含该非信任数据的网页。

3.
在页面生成过程中，应用程序没有阻止数据去包含Web浏览器可执行的内容，如JavaScript、HTML标记、HTML属性、鼠标事件、Flash、ActiveX等。

4. 受害者通过Web浏览器访问生成的网页，其中包含使用非信任数据所注入的恶意脚本。

5.
由于该脚本来自于Web服务器所发送网页，因此受害者的Web浏览器是在Web服务器的域范围内执行恶意脚本。

6.
这从本质上违背了Web浏览器相同来源策略的意图，该策略规定，在一个域中的脚本不应能在不同域够中访问资源或运行代码。

主要有三种类型的跨站脚本：

类型1：反射类XSS（或非持久XSS）

服务器直接从HTTP请求读取数据，并将其反射在HTTP响应中。当攻击者诱使受害者向脆弱的Web应用程序提供危险内容时，就会发生反射XSS攻击，然后反射回受害者，并通过Web浏览器执行。提供恶意内容最常见的机制是将该内容作为一个参数包含在公开发送给或直接通过邮件发送给受害者的URL中。以这种方式构造的URL构成了众多的钓鱼计划的核心，使攻击者能够说服受害者访问引向脆弱网站的网址。在该网站将攻击者的内容反射回被攻击者后，该内容就会被受害者的浏览器所执行。

类型2：存储类XSS（或持续XSS）

应用程序在数据库、消息论坛、访客日志或其它可信的数据存储中存储危险数据。该危险数据随后被读回到应用程序，并被包含在动态内容中。从攻击者的角度看，注入恶意内容的最佳位置是能够展示

给众多用户的区域或是展示给特别用户的区域。特定的用户通常都具有应用程序中的较高权限，或能够接触到对攻击者有价值的敏感数据。如果这样的用户执行恶意内容，那么攻击者就可能可以代表该用户执行特权操作或获取属于该用户的访问敏感数据的权力。例如，攻击者可能会向日志消息中注入XSS，但在管理员查看该日志的时候，可能并没有对其进行妥善处理。

类型0：基于DOM的XSS攻击

在基于DOM的XSS攻击中，客户端将XSS注入到页面中;在其他类型中是由服务器执行注入。基于DOM的XSS一般涉及被发送给客户的、受服务器控制的、值得信赖的脚本，如JavaScript，在客户提高表单之前，JavaScript对该表单执行安全检查。如果服务器提供的脚本处理用户提供的数据，然后将数据注入到网页中（如动态HTML），那么就可能发生基于DOM的XSS攻击。

一旦恶意脚本被注入，攻击者就可以执行各种恶意活动了。攻击者可能会将其中可能包括会话信息cookie之类的私人信息从受害者的机器转移到攻击者机器上。攻击者可以代表受害者向网站发送恶意请求，如果受害者具有管理该网站的管理员权限，那么这种作法对于该网站是尤其危险的。网络钓鱼攻击可以用来模拟信任网站，诱骗受害者输入密码，让攻击者能够危及受害人在该网站上的帐户。最后，该脚本还可能Web浏览器本身的漏洞，从而接管受害者的机器，这种操作有时也被称为“黑客操作”。

在多数情况下，受害者可能根本意识不到受到攻击。面对细心的用户，攻击者经常使用多种方法来对攻击的恶意部分进行编码，如URL编码或Unicode，这样让请求看起来不太可疑。

其它称谓

XSS

CSS: “CSS”曾被作为该漏洞的缩写，但这一缩写会引起与“层叠样式表”之间的混淆，所以对于该缩写的使用已大为下降。

引入阶段

- 架构与设计阶段
- 实现阶段

适用平台

语言

语言无关性

架构范例

基于Web的：*（常用）*

技术类

Web-Server: *（常用）*

平台注释

由于需要进行大量的开发训练才能避免XSS漏洞，因此该漏洞在web应用程序中非常常见。

常见后果

范围	效果
机密性	由跨站脚本造成的最常见攻击一般为披露存储在用户cookie的信息。通常情况下，恶意用户会创建一个客户端脚本，在网络浏览器对其进行分析时，该脚本会执行某些活动（例如向某一E-mail地址发送所有网站的Cookie）。该脚本就会被加载，并且每一个访问该网站的用户都会对它进行运行。由于要求运行该脚本网站可以访问有问题的Cookie，因此恶意脚本也可以对其进行访问。
访问控制	在某些情况下，当跨站点脚本与其他漏洞同时存在时，有可能在受害者的计算机上运行任意代码。
机密性 完整性 可用性	无论是存储型还是反射型，XSS攻击的后果都是一样的。其不同之处在于有效载荷如何到达服务器。 XSS攻击可能会给最终用户带很各种麻烦，其严重程度从产生困扰直到毁掉整个帐户。某些跨站脚本漏洞可以被利用来操纵或窃取cookie，创建有效用户可能被误认为正确的请求，损坏机密信息，或出于不可各种不可告人的目的，在最终用户系统上执行恶意代码。其它破坏性攻击还包括披露最终用户的信息文件，安装木马程序，将用户重定向到其他页面或网站，（在Microsoft Internet Explorer中）运行来自用户认为可信网站上的“Active X”控件，并修改介绍的内容。

被利用的可能性

高到非常高

被利用的原因

跨站脚本攻击可能出现在所有恶意用户被允许向可信网站发布未经校准的材料，让其它有效用户使用，这些常见的地方包括提供基于Web邮件列表样式功能的公告板网站等。

存储类XSS攻击最开始是始于向访客提供“留言”功能的网站。攻击者将JavaScript包含在其留言簿条目中，之后所有访问该留言页的访客都会执行这一恶意代码。如上述示例所显示，XSS漏洞是由在HTTP响应中包含有未经验证数据的代码所引起的。

检测方法

自动静态分析

使用针对这种类型漏洞的自动静态分析工具。许多现代技术都使用数据流分析，来最大限度地减少误报数量。其实这并不是一个完美的解决方案，因为100%的准确率和覆盖率是无法实现的，尤其在涉及到多个组件的时候。

效率：中等

黑盒子方法

使用XSS欺骗表单[REF-14]或自动测试生成工具帮助攻击者发动针对您Web应用程序的多种攻击。该欺骗表单中包含了许多微妙的专门针对XSS防御薄弱系统的XSS变化形式。

效率：中等

关于存储类XSS攻击，由数据存储所造成的间接会导致更加难以发现问题。测试人员必须首先向数据存储中注入XSS字符串，然后找到可以发送XSS字符串到程序其它用户的合适的应用程序功能。这是两个不同的步骤，其中在XSS被最初注入到数据存储中以后，XSS攻击的激活可能需要分钟、几小时甚至几天。

示例

示例1

该示例中涵盖了反射类XSS（类型1）的情况。

下面的JSP代码段从HTTP请求中读取了一个员工ID、eid，并将其显示给用户。

(Bad Code)

Example Language: **JSP**

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

下列ASP.NET代码段从HTTP请求中读取了一个员工ID，并将其显示给用户。

(Bad Code)

Example Language: **ASP.NET**

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

如果员工ID变量只包含标准的字母数字文本，那么在本示例中的代码就可以正常运行。如果其中含有包含元字符或源代码的值，那么该代码在显示HTTP响应的同时就会被Web浏览器执行。最初，可能显现出来的并不像一个漏洞。但，为什么会有人输入一个会导致自己的计算机上运行恶意代码的网址呢？其真正的危险是，攻击者会创建恶意的URL，然后使用电子邮件或社会工程技巧，引诱受害者访问URL链接。当受害者点击该链接时，他们就会不知不觉地通过脆弱的Web应用程序将恶意内容反射到自己的电脑中了。

示例2

该示例中涵盖了反射类XSS（类型2）的情况。

下列JSP代码段使用给定的ID查询员工数据库，并打印出相应的员工姓名。

(Bad Code)

Example Language: **JSP**

```
<%
```

```
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
%>

Employee Name: <%= name %>
```

下列ASP.NET代码段使用给定的ID查询员工数据库，并根据该ID打印出相应的员工姓名。

(Bad Code)

Example Language: **ASP.NET**

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

该代码看起来可能并不危险，因为name的值是从数据库读取的，其内容显然受应用程序的管理。但是，如果name的值来源于用户提供的数据，那么数据库就可能成为提供恶意内容的渠道。如果不对存储在数据库中的所有数据进行正确的输入验证，那么攻击者就可能在用户的Web浏览器中执行恶意命令。

已发现示例

参考	描述
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.
CVE-2008-	Stored XSS in a security product.

0971	
CVE-2008-5249	Stored XSS using a wiki page.
CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

可能的漏洞的消除办法

阶段：架构与设计阶段

策略：库或框架

使用经过审批的库或框架，不允许该漏洞出现或能够提供可以更容易避免这一漏洞的架构。

现有若干有关库和框架可以更容易生成编码正确的输出数据的示例，其中包括微软的反XSS库、OWASP的ESAPI编码模块和Apache Wicket等。

阶段：实现阶段；架构与设计阶段

了解您数据将被使用的环境以及需要进行的编码。当需要在不同组件之间传递数据时，或像网页或多部分邮件消息等在生成的输出数据中同时包含有多个编码时，这一点就显得尤为重要。所有的研究都期望通信协议和数据表示能够确定所需的编码策略。

对于可能成为另一网页输出数据的任何数据来说，尤其是对于通过外部输入数据接收到的数据来说，应针对所有的非字母数字字符进行适当的编码。

同一输出文件不同部分可能需要进行不同的编码，其不同取决于输出数据存在于下列哪个部分：

- HTML正文
- 元素的属性（如SRC = “XYZ” ）
- URIs
- JavaScript部分
- 层叠样式表和样式属性，等。

请注意，HTML实体编码只适用于HTML正文。

咨询XSS Prevention Cheat Sheet[REF- 16]，获取更多有关编码和转义的细节。

阶段：架构与设计阶段

对于客户端上执行的所有安全检查，应确保这些检查在服务器端再次执行，来避免CWE-602的出现。攻击者可以通过在检查后修改值，或更改客户端完全删除客户端检查，来绕过客户端的

检查。然后，这些修改后的值将被提交给服务器。

阶段：实现阶段

使用并指定像ISO- 8859 -1或UTF –
8这样的较强字符编码。如果对编码进行指定，那么Web浏览器就可以猜测网页实际上使用的编码来选择不同的编码。这样您就可能受到与该编码相关的微妙的XSS攻击。参见 CWE-
116来了解更多的编码/转义信息。

阶段：实现阶段

使用Struts，您应将bean的过滤属性设置为true，然后再编写该表单bean的所有数据。

阶段：实现阶段

为了消除针对用户会话cookie的XSS攻击，将会话cookie设置为HttpOnly。在支持HttpOnly功能（如较新版本的Internet
Explorer和Firefox）的浏览器中，该属性可以阻止使用document.cookie的恶意客户端脚本对于用户会话cookie的访问。但由于关不是所有的浏览器都支持HttpOnly，所以这并不是一个完整的解决方案。更重要的是，XMLHttpRequest和其他强大的浏览器技术允许对HTTP标头的读取访问，包括对HttpOnly标志进行设置的Set – Cookie header。

阶段：实现阶段

策略：输入验证

假定所有输入都是恶意的。使用“接受已知良好”的输入验证策略，即使用严格符合规格的可接受输入的白名单。拒绝不完全符合规格的所有输入，或将其转化为完全符合规格的情况。不要单纯依赖对于恶意或有缺陷输入（即不要依赖黑名单）的查找。但，黑名单可用于检测潜在攻击或者确定哪些输入有缺陷应该被断然拒绝。

当执行输入验证时，应考虑所有可能的相关属性，包括长度、输入类型、可接受值的范围、丢失或额外输入、语法、相关领域的连贯性以及业务规则的符合程序。以业务规则逻辑为例，“boat”可能语法上是有效的，因为它仅包含字母数字字符，但如果您期待颜色如“红色”或“蓝色”之类的信息，它就是无效的。

当动态构建网页时，应使用可以对根据请求中预期参数值设置的字符串进行严格限制的白名单。应对所有的输入数据进行验证和清洗，不仅仅是针对用户须指定的那些参数，而且针对请求中的所有数据，包括隐藏字段、cookie、header、URL本身，等等。可能导致持续XSS漏洞的一个常见??错误是只对那些需要被网站反复演示的字段进行验证。我们经常可以看到来自由应用程序服务器所反射请求的数据，或来自于开发团队事先没有预料到的应用程序。此外，未受到充分反射的字段可能被用于未来的开发过程。因此，我们建议对HTTP请求的所有部分进行验证。

请注意，尽管输入验证可能会提供一些纵深??防御，但正确的输出编码、转义和引用仍是防止XSS漏洞最有效的解决方案。这是因为它们可以有效地限制输出数据中会出现的内容。输入验证做不到百分

之百阻止XSS漏洞，特别是当您需要支持可能包含任意字符的自由格式文本字段的时候。例如，在一个聊天应用程序中，因为心表情符号（ “<3” ）很常用，所以很可能会通过验证步骤。但是，它不能被直接插入到网页中，因为其中包含有“<”字符，这将需要进行转义或进行其它处理。在这种情况下，去掉“<”可能会降低XSS风险，但因为表情符号不会被记录下来，所以这样做会产生不正确行为。这看起来会带来一个小小的不便，但，在想要展示不等式的数学论坛中就非常重要了。

即使您在验证过程中犯了一个错误在验证（如忘记1/100的输入字段），适当的编码仍然可能保护您不受注入式攻击。只要输入验证不是孤立进行的，就仍然是一项有用的技术，因为它可以显着降低攻击面，让您能够发现攻击并获得正确编码所不提供的其它安全优势。

一定要在应用程序的明确界面上执行输入验证。这将有助于保护应用程序，即使在某一个数据被重复使用或被移至别处的情况下也是这样。

阶段：使用阶段

使用可以检测攻击该漏洞的应用程序防火墙。这可能无法捕捉到所有的攻击，而且，可能需要进行大量的定制工作。但，在全面的软件安全措施都已部署的情况下，如果代码无法修复（由于受到第三方控制），那么作为一项紧急预防措施这样做就是很有意义的，这样做也有助于提供纵深防御。

详细背景信息

同源策略

同源策略规定，浏览器应该对在可以接触到与客户端网站相关的资源的某一特定网站、或“来源”上运行脚本所能访问的资源进行限制，这一网站或“来源”不应是任何网站或“来源”的客户端资源。该策略旨在阻止网站被修改或读取无关网站的内容。由于万维网涉及许多网站之间的相互作用，因此浏览器必须要执行该策略。

域名

在指XSS攻击时，一个网站的域名大致相当于在该连接的客户一端相关的资源。也就是说，域可以被认为是浏览器存储的用地用户与该网站互动的所有资源。

漏洞出现的次序

次序	描述
结果性漏洞	*（该漏洞的出现取决于其它漏洞是否存在）*

关系

性质	类型	ID	名称		
ChildOf		20	Improper Input Validation	**700**	
ChildOf		74	Failure to Sanitize Data into a Different Plane ('Injection')	**699** **1000**	
ChildOf		442	Web Problems	699	
ChildOf		712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	**629**	

ChildOf		722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	711	
ChildOf		725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	**711**	
ChildOf		751	2009 Top 25 - Insecure Interaction Between Components	**750**	
ChildOf		801	2010 Top 25 - Insecure Interaction Between Components	**800**	
CanPrecede		494	Download of Code Without Integrity Check	1000	
PeerOf		352	Cross-Site Request Forgery (CSRF)	1000	
ParentOf		80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	**699** **1000**	
ParentOf		81	Improper Sanitization of Script in an Error Message Web Page	**699** **1000**	
ParentOf		83	Improper Neutralization of Script in Attributes in a Web Page	**699** **1000**	
ParentOf		84	Failure to Resolve Encoded URI Schemes in a Web Page	**699** **1000**	
ParentOf		85	Doubled Character XSS Manipulations	**699** **1000**	
ParentOf		86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	**699** **1000**	
ParentOf		87	Failure to Sanitize Alternate XSS Syntax	**699** **1000**	
MemberOf		635	Weaknesses Used by NVD	**635**	
CanFollow		113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	1000	
CanFollow		184	Incomplete Blacklist	1000	692

f 成因性质

明示

缺陷类别映射

映射分类	节点	适用于	映射节点名称
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)

OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

相关的攻击模式

CAPEC-ID	攻击模式名称	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

参考

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <http://ha.ckers.org/xss.html>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <http://msdn.microsoft.com/en-us/library/ms533046.aspx>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>.

"OWASP Enterprise Security API (ESAPI) Project". <http://www.owasp.org/index.php/ESAPI>.

Ivan Ristic. "XSS Defense HOWTO". <http://blog.modsecurity.org/2008/07/do-you-know-how.html>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHTTPRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <http://wicket.apache.org/>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	PLOVER		Externally Mined
修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Observed Examples, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples		
2010-02-	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Detection Factors, Potential		

16	Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Description, Potential Mitigations, Related Attack Patterns		

相关历史条目	
更改日期	**相关历史条目**
2008-04-11	跨站脚本 (XSS)
2009-01-12	未能对网页中的指令进行消毒（即“跨站脚本攻击”）
2009-05-27	未能维护网页结构（即“跨站脚本”）

BACK TO TOP

Failure to Preserve Web Page Structure ('Cross-site Scripting')

Weakness **Status:** Usable

ID: 79 (Weakness Base)

描述

简要描述

该软件没有对用户可控的输入数据进行充分验证、过滤、避免和/或Encode，就将其放在输出数据中，用于WEB页面服务于其他用户。

扩展描述

当下列情况发生时，出现跨站脚本（XSS）漏洞：

1. 非信任的数据进入Web应用程序中，这样的数据通常来自于Web请求。

2. Web应用程序动态生成一个包含该非信任数据的网页。

3.
在页面生成过程中，应用程序没有阻止数据去包含Web浏览器可执行的内容，如JavaScript、HTML标记、HTML属性、鼠标事件、Flash、ActiveX等。

4. 受害者通过Web浏览器访问生成的网页，其中包含使用非信任数据所注入的恶意脚本。

5.
由于该脚本来自于Web服务器所发送网页，因此受害者的Web浏览器是在Web服务器的域范围内执行恶意脚本。

6.
这从本质上违背了Web浏览器相同来源策略的意图，该策略规定，在一个域中的脚本不应能在不同域够中访问资源或运行代码。

主要有三种类型的跨站脚本：

类型1：反射类XSS（或非持久XSS）

服务器直接从HTTP请求读取数据，并将其反射在HTTP响应中。当攻击者诱使受害者向脆弱的Web应用程序提供危险内容时，就会发生反射XSS攻击，然后反射回受害者，并通过Web浏览器执行。提供恶意内容最常见的机制是将该内容作为一个参数包含在公开发送给或直接通过邮件发送给受害者的URL中。以这种方式构造的URL构成了众多的钓鱼计划的核心，使攻击者能够说服受害者访问引向脆弱网站的网址。在该网站将攻击者的内容反射回被攻击者后，该内容就会被受害者的浏览器所执行。

类型2：存储类XSS（或持续XSS）

应用程序在数据库、消息论坛、访客日志或其它可信的数据存储中存储危险数据。该危险数据随后被读回到应用程序，并被包含在动态内容中。从攻击者的角度看，注入恶意内容的最佳位置是能够展示

给众多用户的区域或是展示给特别用户的区域。特定的用户通常都具有应用程序中的较高权限，或能够接触到对攻击者有价值的敏感数据。如果这样的用户执行恶意内容，那么攻击者就可能可以代表该用户执行特权操作或获取属于该用户的访问敏感数据的权力。例如，攻击者可能会向日志消息中注入XSS，但在管理员查看该日志的时候，可能并没有对其进行妥善处理。

类型0：基于DOM的XSS攻击

在基于DOM的XSS攻击中，客户端将XSS注入到页面中;在其他类型中是由服务器执行注入。基于DOM的XSS一般涉及被发送给客户的、受服务器控制的、值得信赖的脚本，如JavaScript，在客户提高表单之前，JavaScript对该表单执行安全检查。如果服务器提供的脚本处理用户提供的数据，然后将数据注入到网页中（如动态HTML），那么就可能发生基于DOM的XSS攻击。

一旦恶意脚本被注入，攻击者就可以执行各种恶意活动了。攻击者可能会将其中可能包括会话信息cookie之类的私人信息从受害者的机器转移到攻击者机器上。攻击者可以代表受害者向网站发送恶意请求，如果受害者具有管理该网站的管理员权限，那么这种作法对于该网站是尤其危险的。网络钓鱼攻击可以用来模拟信任网站，诱骗受害者输入密码，让攻击者能够危及受害人在该网站上的帐户。最后，该脚本还可能Web浏览器本身的漏洞，从而接管受害者的机器，这种操作有时也被称为“黑客操作”。

在多数情况下，受害者可能根本意识不到受到攻击。面对细心的用户，攻击者经常使用多种方法来对攻击的恶意部分进行编码，如URL编码或Unicode，这样让请求看起来不太可疑。

其它称谓

XSS

CSS: “CSS”曾被作为该漏洞的缩写，但这一缩写会引起与“层叠样式表”之间的混淆，所以对于该缩写的使用已大为下降。

引入阶段

- 架构与设计阶段
- 实现阶段

适用平台

语言

语言无关性

架构范例

基于Web的：*（常用）*

技术类

Web-Server: *（常用）*

平台注释

由于需要进行大量的开发训练才能避免XSS漏洞，因此该漏洞在web应用程序中非常常见。

常见后果

范围	效果
机密性	由跨站脚本造成的最常见攻击一般为披露存储在用户cookie的信息。通常情况下，恶意用户会创建一个客户端脚本，在网络浏览器对其进行分析时，该脚本会执行某些活动（例如向某一E-mail地址发送所有网站的Cookie）。该脚本就会被加载，并且每一个访问该网站的用户都会对它进行运行。由于要求运行该脚本网站可以访问有问题的Cookie，因此恶意脚本也可以对其进行访问。
访问控制	在某些情况下，当跨站点脚本与其他漏洞同时存在时，有可能在受害者的计算机上运行任意代码。
机密性 完整性 可用性	无论是存储型还是反射型，XSS攻击的后果都是一样的。其不同之处在于有效载荷如何到达服务器。 XSS攻击可能会给最终用户带很各种麻烦，其严重程度从产生困扰直到毁掉整个帐户。某些跨站脚本漏洞可以被利用来操纵或窃取cookie，创建有效用户可能被误认为正确的请求，损坏机密信息，或出于不可各种不可告人的目的，在最终用户系统上执行恶意代码。其它破坏性攻击还包括披露最终用户的信息文件，安装木马程序，将用户重定向到其他页面或网站，（在Microsoft Internet Explorer中）运行来自用户认为可信网站上的“Active X”控件，并修改介绍的内容。

被利用的可能性

高到非常高

被利用的原因

跨站脚本攻击可能出现在所有恶意用户被允许向可信网站发布未经校准的材料，让其它有效用户使用，这些常见的地方包括提供基于Web邮件列表样式功能的公告板网站等。

存储类XSS攻击最开始是始于向访客提供“留言”功能的网站。攻击者将JavaScript包含在其留言簿条目中，之后所有访问该留言页的访客都会执行这一恶意代码。如上述示例所显示，XSS漏洞是由在HTTP响应中包含有未经验证数据的代码所引起的。

检测方法

自动静态分析

使用针对这种类型漏洞的自动静态分析工具。许多现代技术都使用数据流分析，来最大限度地减少误报数量。其实这并不是一个完美的解决方案，因为100%的准确率和覆盖率是无法实现的，尤其在涉及到多个组件的时候。

效率：中等

黑盒子方法

使用XSS欺骗表单[REF-14]或自动测试生成工具帮助攻击者发动针对您Web应用程序的多种攻击。该欺骗表单中包含了许多微妙的专门针对XSS防御薄弱系统的XSS变化形式。

效率：中等

关于存储类XSS攻击，由数据存储所造成的间接会导致更加难以发现问题。测试人员必须首先向数据存储中注入XSS字符串，然后找到可以发送XSS字符串到程序其它用户的合适的应用程序功能。这是两个不同的步骤，其中在XSS被最初注入到数据存储中以后，XSS攻击的激活可能需要分钟、几小时甚至几天。

示例

示例1

该示例中涵盖了反射类XSS（类型1）的情况。

下面的JSP代码段从HTTP请求中读取了一个员工ID、eid，并将其显示给用户。

(Bad Code)

Example Language: **JSP**

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

下列ASP.NET代码段从HTTP请求中读取了一个员工ID，并将其显示给用户。

(Bad Code)

Example Language: **ASP.NET**

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

如果员工ID变量只包含标准的字母数字文本，那么在本示例中的代码就可以正常运行。如果其中含有包含元字符或源代码的值，那么该代码在显示HTTP响应的同时就会被Web浏览器执行。最初，可能显现出来的并不像一个漏洞。但，为什么会有人输入一个会导致自己的计算机上运行恶意代码的网址呢？其真正的危险是，攻击者会创建恶意的URL，然后使用电子邮件或社会工程技巧，引诱受害者访问URL链接。当受害者点击该链接时，他们就会不知不觉地通过脆弱的Web应用程序将恶意内容反射到自己的电脑中了。

示例2

该示例中涵盖了反射类XSS（类型2）的情况。

下列JSP代码段使用给定的ID查询员工数据库，并打印出相应的员工姓名。

(Bad Code)

Example Language: **JSP**

```
<%
```

```
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
%>

Employee Name: <%= name %>
```

下列ASP.NET代码段使用给定的ID查询员工数据库，并根据该ID打印出相应的员工姓名。

(Bad Code)

Example Language: **ASP.NET**

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

该代码看起来可能并不危险，因为name的值是从数据库读取的，其内容显然受应用程序的管理。但是，如果name的值来源于用户提供的数据，那么数据库就可能成为提供恶意内容的渠道。如果不对存储在数据库中的所有数据进行正确的输入验证，那么攻击者就可能在用户的Web浏览器中执行恶意命令。

已发现示例

参考	描述
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.
CVE-2008-	Stored XSS in a security product.

0971	
CVE-2008-5249	Stored XSS using a wiki page.
CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

可能的漏洞的消除办法

阶段：架构与设计阶段

策略：库或框架

使用经过审批的库或框架，不允许该漏洞出现或能够提供可以更容易避免这一漏洞的架构。

现有若干有关库和框架可以更容易生成编码正确的输出数据的示例，其中包括微软的反XSS库、OWASP的ESAPI编码模块和Apache Wicket等。

阶段：实现阶段；架构与设计阶段

了解您数据将被使用的环境以及需要进行的编码。当需要在不同组件之间传递数据时，或像网页或多部分邮件消息等在生成的输出数据中同时包含有多个编码时，这一点就显得尤为重要。所有的研究都期望通信协议和数据表示能够确定所需的编码策略。

对于可能成为另一网页输出数据的任何数据来说，尤其是对于通过外部输入数据接收到的数据来说，应针对所有的非字母数字字符进行适当的编码。

同一输出文件不同部分可能需要进行不同的编码，其不同取决于输出数据存在于下列哪个部分：

- HTML正文
- 元素的属性（如SRC = “XYZ” ）
- URIs
- JavaScript部分
- 层叠样式表和样式属性，等。

请注意，HTML实体编码只适用于HTML正文。

咨询XSS Prevention Cheat Sheet[REF- 16]，获取更多有关编码和转义的细节。

阶段：架构与设计阶段

对于客户端上执行的所有安全检查，应确保这些检查在服务器端再次执行，来避免CWE-602的出现。攻击者可以通过在检查后修改值，或更改客户端完全删除客户端检查，来绕过客户端的

检查。然后，这些修改后的值将被提交给服务器。

阶段：实现阶段

使用并指定像ISO- 8859 -1或UTF –
8这样的较强字符编码。如果对编码进行指定，那么Web浏览器就可以猜测网页实际上使用的编码来选择不同的编码。这样您就可能受到与该编码相关的微妙的XSS攻击。参见 CWE-
116来了解更多的编码/转义信息。

阶段：实现阶段

使用Struts，您应将bean的过滤属性设置为true，然后再编写该表单bean的所有数据。

阶段：实现阶段

为了消除针对用户会话cookie的XSS攻击，将会话cookie设置为HttpOnly。在支持HttpOnly功能（如较新版本的Internet
Explorer和Firefox）的浏览器中，该属性可以阻止使用document.cookie的恶意客户端脚本对于用户会话cookie的访问。但由于关不是所有的浏览器都支持HttpOnly，所以这并不是一个完整的解决方案。更重要的是，XMLHttpRequest和其他强大的浏览器技术允许对HTTP标头的读取访问，包括对HttpOnly标志进行设置的Set – Cookie header。

阶段：实现阶段

策略：输入验证

假定所有输入都是恶意的。使用“接受已知良好”的输入验证策略，即使用严格符合规格的可接受输入的白名单。拒绝不完全符合规格的所有输入，或将其转化为完全符合规格的情况。不要单纯依赖对于恶意或有缺陷输入（即不要依赖黑名单）的查找。但，黑名单可用于检测潜在攻击或者确定哪些输入有缺陷应该被断然拒绝。

当执行输入验证时，应考虑所有可能的相关属性，包括长度、输入类型、可接受值的范围、丢失或额外输入、语法、相关领域的连贯性以及业务规则的符合程序。以业务规则逻辑为例，“boat”可能语法上是有效的，因为它仅包含字母数字字符，但如果您期待颜色如“红色”或“蓝色”之类的信息，它就是无效的。

当动态构建网页时，应使用可以对根据请求中预期参数值设置的字符串进行严格限制的白名单。应对所有的输入数据进行验证和清洗，不仅仅是针对用户须指定的那些参数，而且针对请求中的所有数据，包括隐藏字段、cookie、header、URL本身，等等。可能导致持续XSS漏洞的一个常见??错误是只对那些需要被网站反复演示的字段进行验证。我们经常可以看到来自由应用程序服务器所反射请求的数据，或来自于开发团队事先没有预料到的应用程序。此外，未受到充分反射的字段可能被用于未来的开发过程。因此，我们建议对HTTP请求的所有部分进行验证。

请注意，尽管输入验证可能会提供一些纵深??防御，但正确的输出编码、转义和引用仍是防止XSS漏洞最有效的解决方案。这是因为它们可以有效地限制输出数据中会出现的内容。输入验证做不到百分

之百阻止XSS漏洞，特别是当您需要支持可能包含任意字符的自由格式文本字段的时候。例如，在一个聊天应用程序中，因为心表情符号（ “<3” ）很常用，所以很可能会通过验证步骤。但是，它不能被直接插入到网页中，因为其中包含有“<”字符，这将需要进行转义或进行其它处理。在这种情况下，去掉“<”可能会降低XSS风险，但因为表情符号不会被记录下来，所以这样做会产生不正确行为。这看起来会带来一个小小的不便，但，在想要展示不等式的数学论坛中就非常重要了。

即使您在验证过程中犯了一个错误在验证（如忘记1/100的输入字段），适当的编码仍然可能保护您不受注入式攻击。只要输入验证不是孤立进行的，就仍然是一项有用的技术，因为它可以显着降低攻击面，让您能够发现攻击并获得正确编码所不提供的其它安全优势。

一定要在应用程序的明确界面上执行输入验证。这将有助于保护应用程序，即使在某一个数据被重复使用或被移至别处的情况下也是这样。

阶段：使用阶段

使用可以检测攻击该漏洞的应用程序防火墙。这可能无法捕捉到所有的攻击，而且，可能需要进行大量的定制工作。但，在全面的软件安全措施都已部署的情况下，如果代码无法修复（由于受到第三方控制），那么作为一项紧急预防措施这样做就是很有意义的，这样做也有助于提供纵深防御。

详细背景信息

同源策略

同源策略规定，浏览器应该对在可以接触到与客户端网站相关的资源的某一特定网站、或“来源”上运行脚本所能访问的资源进行限制，这一网站或“来源”不应是任何网站或“来源”的客户端资源。该策略旨在阻止网站被修改或读取无关网站的内容。由于万维网涉及许多网站之间的相互作用，因此浏览器必须要执行该策略。

域名

在指XSS攻击时，一个网站的域名大致相当于在该连接的客户一端相关的资源。也就是说，域可以被认为是浏览器存储的用地用户与该网站互动的所有资源。

漏洞出现的次序

次序	描述
结果性漏洞	*（该漏洞的出现取决于其它漏洞是否存在）*

关系

性质	类型	ID	名称		
ChildOf		20	Improper Input Validation	**700**	
ChildOf		74	Failure to Sanitize Data into a Different Plane ('Injection')	**699** **1000**	
ChildOf		442	Web Problems	699	
ChildOf		712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	**629**	

ChildOf		722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	711	
ChildOf		725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	**711**	
ChildOf		751	2009 Top 25 - Insecure Interaction Between Components	**750**	
ChildOf		801	2010 Top 25 - Insecure Interaction Between Components	**800**	
CanPrecede		494	Download of Code Without Integrity Check	1000	
PeerOf		352	Cross-Site Request Forgery (CSRF)	1000	
ParentOf		80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	**699** **1000**	
ParentOf		81	Improper Sanitization of Script in an Error Message Web Page	**699** **1000**	
ParentOf		83	Improper Neutralization of Script in Attributes in a Web Page	**699** **1000**	
ParentOf		84	Failure to Resolve Encoded URI Schemes in a Web Page	**699** **1000**	
ParentOf		85	Doubled Character XSS Manipulations	**699** **1000**	
ParentOf		86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	**699** **1000**	
ParentOf		87	Failure to Sanitize Alternate XSS Syntax	**699** **1000**	
MemberOf		635	Weaknesses Used by NVD	**635**	
CanFollow		113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	1000	
CanFollow		184	Incomplete Blacklist	1000	692

f 成因性质

明示

缺陷类别映射

映射分类	节点	适用于	映射节点名称
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)

OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

相关的攻击模式

CAPEC-ID	攻击模式名称	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

参考

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <http://ha.ckers.org/xss.html>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <http://msdn.microsoft.com/en-us/library/ms533046.aspx>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>.

"OWASP Enterprise Security API (ESAPI) Project". <http://www.owasp.org/index.php/ESAPI>.

Ivan Ristic. "XSS Defense HOWTO". <http://blog.modsecurity.org/2008/07/do-you-know-how.html>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHTTPRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <http://wicket.apache.org/>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	PLOVER		Externally Mined
修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Observed Examples, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples		
2010-02-	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Detection Factors, Potential		

16	Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Description, Potential Mitigations, Related Attack Patterns		

相关历史条目	
更改日期	**相关历史条目**
2008-04-11	跨站脚本 (XSS)
2009-01-12	未能对网页中的指令进行消毒（即“跨站脚本攻击”）
2009-05-27	未能维护网页结构（即“跨站脚本”）

BACK TO TOP

对SQL命令中使用的特殊元素进行的不正确消毒处理（SQL注入）

Weakness **Status**

ID: 89 (Weakness Base) **:** Draft

描述

简要描述

软件使用来自上游组件,并受外部影响的输入数据构造SQL命令的全部或一部分，但它并没有清洁或者正确清洁特定的元素,当这些元素被SQL
命令使用时,可能会修改SQL命令的本意,从而危及数据库的安全。

扩展描述

如果没有对用户可控的输入数据中的SQL字符串进行充分的验证，那么所生成的SQL查询可能会导致这些输入数据被解释为SQL命令而不是普通用户的输入数据。攻击者就可能对此加以利用来更改查询逻辑,从而绕过安全检查，或插入可以更改后端数据库的额外语句，可能包括执行操作系统命令。

SQL注入已成为数据库驱动网站上常见的问题。这个漏洞很容易被发现，并且容易被利用，因此，即使仅有很小用户的网站或软件包都有可能受到这种攻击。

引入阶段

- 架构与设计阶段
- 实现阶段
- 使用阶段

适用平台

语言

所有

技术类别

数据库服务器

引入模式

这一漏洞通常出现在数据库中保存用户输入的数据丰富的应用程序中。

常见后果

范围	效果
机密性	由于SQL数据库中通常存有敏感数据，因此机密性损失通常是伴随SQL注入漏洞同时存在的问题。

身份认证	如果使用弱SQL命令来检查用户名和密码，那么在就有可能在另一个用户不知道密码的情况下连接到系统中。
授权	如果授权的信息保存在SQL数据库，就有可能通过利用SQL注入的漏洞更改该信息。
完整性	正如有可能读取敏感信息，因此也可以利用SQL注入攻击对此信息进行修改、甚至删除。

被利用的可能性

非常高

被利用的原因

应用程序动态生成包含用户输入的查询。

检测方法

自动静态分析

使用自动静态分析工具通常可以检测到该漏洞。许多现代工具使用数据流分析或约束型技术来减少误报数量。

如果执行的是正确的输入验证，那么自动静态分析就可能无法识别该漏洞，从而导致误报的发生- 即产生没有任何安全后果也不需要修改任何代码的警告。

自动静态分析可能无法检测到是否使用了定制的API函数或间接调用SQL命令的第三方库，从而导致有漏洞未报的情况- 特别是在没有API/库代码供分析的情况下更是这样。

人工分析

人工分析有助于发现这一漏洞，但在有限的时间内可能无法达到预期的代码覆盖率。鉴于攻击面可能过大，所以如果为这一漏洞要考虑所有输入数据，那么操作起来就很困难了。

示例

示例1

2008年，大量Web服务器受到使用相同的SQL注入攻击字符串的损害。这种单一字符串针对许多不同的程序。当时使用 SQL注入来修改网站、服务恶意代码。 [1]

示例2

下面的代码动态地构建并执行搜索匹配指定itemname的SQL查询。要求userName与先前认证通过的用户名相匹配。Itemname与输入itemName.Text相匹配。

(Bad Code)

Example Language: **C#**

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND itemname = '" + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

本代码打算执行的查询遵循：

```
SELECT * FROM items WHERE owner = <userName> AND itemname = <itemName>;
```

但是，由于查询的动态建立是通过连接常量库查询字符串和用户输入的字符串来实现的，因此只有在itemName中不包含单引号字符时，查询才能正确执行。如果用户名为wiley的攻击者输入字符串：

(Attack)

```
name' OR 'a'='a
```

作为itemName，那么查询就会变成：

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

增加的：

(Attack)

```
OR 'a'='a'
```

条件会导致WHERE子句的估值始终为true，因此查询在逻辑上就等同于一个更为简单的查询：

(Attack)

```
SELECT * FROM items;
```

查询的这种简化使攻击者能够绕过查询只返回身份验证合格的用户所拥有的项目的要求；而查询现在所返回的是存储在项目表中的所有条目，不论所有者是谁。

示例3

该示例检查的是前面例子中构建并执行的传递给查询的一个由不同的恶意值所造成的影响有多大。如果用户名为wiley的攻击者输入字符串：

(Attack)

```
name'; DELETE FROM items; --
```

作为itemName，那么该查询就会变成下面两个查询：

(Attack)

Example Language: **SQL**

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
--'
```

许多数据库服务器，其中包括微软(R) SQL Server 2000，都允许被分号分隔的多个SQL语句被同时执行。虽然这种攻击字符串会导致在Oracle和其他不允许批量执行由分号分隔的语句的数据库服务器上执行出错，但在允许分批执行的数据库中，这种类型的攻击仍然允许攻击者对数据库执行任意指令。

应注意尾随的双连字符(--

),其中对大多数的数据库服务器规定，语句的其余部分应被视为一个注释，而不被执行。在这种情况下，注释字符所起的作用是删除被更改的查询所遗留下来的尾随单引号。在这种方法在不允许使用注释的数据库中，使用类似于前例中所示的办法，仍然可以使一般的攻击有效发挥作用。

若攻击者输入字符串

(Attack)

```
name'; DELETE FROM items; SELECT * FROM items WHERE 'a'='a
```

那么就会创建下列三个有效语句：

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
SELECT * FROM items WHERE 'a'='a';
```

一种传统的办法来防止SQL注入攻击就是将它当作一个输入验证问题来处理，要么只接受安全值在白名单中的字符，要么识别并躲开存在潜在恶意值的黑名单。白名单可能是严格执行输入验证规则的一个非常有效的手段，但参数化的SQL语句需要较少的维护，并且能够在安全方面提供更多的保障。黑名单可以说总是充满漏洞，让其无法有效阻止SQL的注入攻击。例如，攻击者可以：

- 找到没被引用的字段
- 设法绕过对于某些避开元字符的需求
- 使用预先写好的存储过程来隐藏注入的元字符

手动将输入数据中的字符转义至SQL查询可以起到帮助的作用，但不能确保应用程序不受SQL注入的攻击。

另一种通常用来处理SQL注入攻击的办法是使用存储过程。虽然存储过程
能够防止某些类型的SQL注入攻击，但还是有许多别的问题防止不了。例如，下面的PL / SQL程序很容易受到和显示在第一个例子中一样的SQL注入攻击。

(Bad Code)

```
procedure get_item ( itm_cv IN OUT ItmCurTyp, usr in varchar2, itm in varchar2)
is open itm_cv for
' SELECT * FROM items WHERE ' || 'owner = '|| usr || ' AND itemname = ' || itm || ';
end get_item;
```

通过限制可以传递给参数的语句的类型，存储过程通常有助于防止SQL注入攻击。然而，仍有很多受限制和有意思的语句绕过存储过程的限制。而且，存储过程可以防止某些漏洞，但不能保证您的应用系统不受SQL注入的攻击。

示例4

MS

SQL具有内置的函数，可以执行shell命令。这种情况中的SQL注入可能是灾难性的。例如，下面表单的查询：

(Bad Code)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='$user_input' ORDER BY PRICE
```

在这里，$user_input 来自于用户，并且没有经过过滤。

如果用户提供的字符串是:

(Attack)

```
' exec master..xp_cmdshell 'vol' --
```

那么查询就会遵循下列形式: "

(Attack)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='' exec master..xp_cmdshell 'vol' --' ORDER BY PRICE
```

现在，此查询可分为:

- [1]第一个SQL查询：SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY=''
- [2]第二个SQL查询，执行一个shell命令：exec master..xp_cmdshell 'vol'
- [3]一个MS SQL注释： --' ORDER BY PRICE

可以看出，恶意输入可以将一个查询的语义变为一个查询、一个shell命令的执行以及注释。

示例5

代码计划根据一个消息ID打印该消息的摘要。

(Bad Code)

Example Language: **PHP**

```
$id = $_COOKIE["mid"];
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

程序员可能假设攻击者无法修改cookie而跳过$输入验证。不过，处理自定义客户端代码或甚至在Web浏览器中都很容易实现。

尽管$ id包裹在以对mysql_query调用的单引号中，但攻击者仍可以将传入的mid cookie简单地变成：

(Attack)

```
1432' or '1' = '1
```

结果将产生查询：

(Result)

```
SELECT MessageID, Subject FROM messages WHERE MessageID = '1432' or '1' = '1'
```

这不仅会检索消息编号1432，还会检索所有其他消息。

在这种情况下，程序员可以对代码进行简单的修改从而消除SQL注入：

(Good Code)

Example Language: **PHP**

```
$id = intval($_COOKIE["mid"]);
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

但，如果该代码旨在支持含有不同消息框的多个用户，那么代码可能还需要进行访问控制检查（CWE-285），来确保应用程序用户有权查看该消息。

示例6

本示例试图获得用户提供的最终名称，并将该名称输入到数据库中。

(Bad Code)

Example Language: **Perl**

```
$userKey = getUserID();
$name = getUserInput();
# ensure only letters, hyphens and apostrophe are allowed
$name = whiteList($name, "^a-zA-z'-$");
$query = "INSERT INTO last_names VALUES('$userKey', '$name')";
```

尽管程序员对用户输入使用了白名单，但这也有缺点。首先，用户仍可以提供在SQL中被作为注释结构的连字符。如果用户进行指定-

那么该语句的其余部分将被视为注释，从而可能会绕过安全逻辑。此外，白名单允许同是SQL中命令分隔数据的单引号。如果用户提供了一个带有撇号的名称，那么就可能能够改变整个语句的结构，甚至改变程序控制流，可能对机密信息进行访问或修改。在这种情况下，单引号和撇号都是用于最终名称的合法字符，必须进行允许操作。相反，程序员可能想使用准备好的语句或对输入数据进行编码程序，从而防止任何数据/指令误解。

已发现的示例

参考	描述
CVE-2004-0366	链：用于数据库认证的库中SQL注入允许SQL注入和绕过认证。
CVE-2008-2790	通过本应是数字标识的SQL注入。
CVE-2008-2223	通过本应是数字标识的SQL注入。
CVE-2007-6602	通过用户名称的SQL注入。
CVE-2008-5817	通过用户名称或密码字段的SQL注入。
CVE-2003-0377	使用精心制作的组名称现安全产品中进行SQL注入。

CVE-2008-2380	向认证库中进行SQL注入。

可能的漏洞消除办法

阶段：架构与设计阶段

策略：使用库或框架

使用不允许该漏洞出现或能够提供可以使本漏洞更容易被避免的已经审查的库或框架。

例如，应考虑使用Hibernate或Enterprise Java Beans等持久层，这样可以较有效地抵御SQL，如果使用得当的话。

阶段：架构与设计阶段

策略：参数化处理

如果可以，使用可自动执行数据与代码分离的结构化机制。这些机制可能能够进行相关的报价、编码、并自动验证，而不是依赖开发人员在每一个有输出数据生成的地方发挥作用。

使用预处理语句、参数化查询或已经参数化的存储过程来处理SQL查询。这些功能须能够接受参数或变量并支持强类型。

```
String userName = ctx.getAuthenticatedUserName();
String itemName = request.getParameter("itemName");
String query = "SELECT * FROM items WHERE itemname=? AND owner=?";
Query stmt = sess.createQuery(query);
stmt.setString(0, itemName);
stmt.setString(1, userName);
List items = stmt.list();
```

不要在这些功能内部使用“exec”或类似功能来动态地构建和执行查询字符串，因为这样您可能又重新引入了SQL注入。

阶段：架构与设计阶段

遵循最低权限原则去创建SQL数据库的用户帐户。该数据库用户应仅拥有使用其帐户所需要的最低权限。如果系统要求显示用户可以读取并修改自己的数据，那么应限制他们的权限，让他们不能读/写别人的数据。尽可能对所有数据库对象使用最严格的权限，如对已存储进程仅有执行权限。

阶段：架构与设计阶段

对于在客户端执行的任何安全检查，应确保这些检查是在服务器端再做一次，以避免CWE-602漏洞。攻击者可通过在检查完成后修改值或通过更改客户端从而完全删除客户端检查来绕过客户端检查。然后，这些修改后的值将被提交给服务器。

阶段：实现阶段

如果无论有什么样的风险，您都需要使用动态生成的查询字符串，那么应使用正确的编码和输入转义。不要建立自己的实现，因为这样的功能可能会在数据库或编程语言中找到。例如，Oracle

DBMS_ASSERT包可以检查或加强参数所具有的使它们不易受到SQL注入攻击的某些特性。对于MySQL，在C和PHP中都可以找到mysql_real_escape_string() API函数。

阶段：实现阶段

策略：输入验证

假定所有输入都是恶意的。使用“接受已知良好”的输入验证策略，即使用严格符合规格的可接受输入的白名单。拒绝不完全符合规格的所有输入，或将其转化为完全符合规格的情况。不要单纯依赖对于恶意或有缺陷输入（即不要依赖黑名单）的查找。但，黑名单可用于检测潜在攻击或者确定哪些输入有缺陷应该被断然拒绝。

当执行输入验证时，应考虑所有可能的相关属性，包括长度、输入类型、可接受值的范围、丢失或额外输入、语法、相关领域的连贯性以及业务规则的符合程序。以业务规则逻辑为例，“boat”可能语法上是有效的，因为它仅包含字母数字字符，但如果您期待颜色如“红色”或“蓝色”之类的信息，它就是无效的。

当构建SQL查询字符串时，应使用可以对根据请求中预期参数值设置的字符串进行严格限制的白名单。这将间接地限制攻击范围，但这种技术没有正确的输出编码和转义更重要。

请注意，尽管输入验证可能会提供一些纵深??防御，但正确的输出编码、转义和引用仍是防止SQL注入最有效的解决方案。这是因为它们可以有效地限制输出数据中会出现的内容。输入验证做不到百分之百阻止SQL注入，特别是当您需要支持可能包含任意字符的自由格式文本字段的时候。例如，名称“O'Reilly”很可能会通过验证，因为这是一个常见的英文姓氏。但，它不能被直接插入到数据库中，因为它包含了“'”撇号字符，这就将需要进行转义或以其他方式处理。在这种情况下，去除撇号可能会降低SQL注入风险，但这会产生不正确的行为，因为所记录的名字就是错误的了。

在可行的情况下，完全禁止元字符而不是对其进行转义可能是最安全的作法。这种作法会提供一些深入防御。在数据被输入数据库以后，后来进程在使用元字符之前可能忘记对其进行转义，而您也可能无法控制这些进程。

阶段：测试、实现阶段

使用针对这种漏洞类型的自动静态分析工具。许多现代技术都是使用数据流分析来尽量降低误报。但由于不可能达到100%的准确率和覆盖率，所以这并不是一个完美的解决方案。

阶段：测试阶段

使用动态的利用大型测试套件处理多种输入的与软件互动的工具和技术，如模糊测试（fuzzing）、坚固性测试、故障注入。软件的操作可以被放缓，但它不应不稳定、崩溃或产生不正确的结果。

阶段：使用阶段

使用可以检测到攻击此漏洞的应用程序防火墙。这可能无法捕捉所有的攻击，而且可能需要进行一些定制工作。但是，在代码无法被修复的情况下（由于代码受第三方控制），在应用更为全面的软件安全保护措施的同时，作为一种紧急事件的预防措施，或用作纵深防御，这种作法都是有益的。

关系

性质	类型	ID	名称	
ChildOf		20	Improper Input Validation	**700**
ChildOf		77	Improper Sanitization of Special Elements used in a Command ('Command Injection')	**699** **1000**
ChildOf		713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**629**
ChildOf		722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	711
ChildOf		727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**711**
ChildOf		751	2009 Top 25 - Insecure Interaction Between Components	**750**
ChildOf		801	2010 Top 25 - Insecure Interaction Between Components	**800**
ParentOf		564	SQL Injection: Hibernate	**699** **1000**
MemberOf		630	Weaknesses Examined by SAMATE	**630**
MemberOf		635	Weaknesses Used by NVD	**635**
CanFollow		456	Missing Initialization	1000

关联说明

SQL注入可能是由于特殊字符管理不善、MAID或黑名单/白名单问题造成的。是首要的身份验证错误。

缺陷类别映射

映射分类	节点	适用于	映射节点名称
PLOVER			SQL injection
7 Pernicious Kingdoms			SQL Injection
CLASP			SQL injection
OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws
WASC	19		SQL Injection

相关的攻击模式

CAPEC-ID	攻击模式名称	*(CAPEC Version: 1.5)*
7	SQL盲注	
66	SQL注入	
108	通过SQL注入执行命令行	

109	对象关系映射注入
110	通过SOAP参数篡改进行SQL注入

白盒定义

通过SOAP参数篡改进行SQL注入

1. 起始语句接受输入

2. 结束语句执行SQL命令，在以下情况下：

a. 输入为SQL命令的一部分

b. 输入中包含SQL句法（尤其是存在有查询分隔符的情况下）

参考

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 1: SQL Injection." Page 3. McGraw-Hill. 2010.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 12, "Database Input Issues" Page 397. 2nd Edition. Microsoft. 2002.

OWASP. "SQL Injection Prevention Cheat Sheet". <http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>.

Steven Friedl. "SQL Injection Attacks by Example". 2007-10-10. <http://www.unixwiz.net/techtips/sql-injection.html>.

Ferruh Mavituna. "SQL Injection Cheat Sheet". 2007-03-15. <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>.

David Litchfield, Chris Anley, John Heasman and Bill Grindlay. "The Database Hacker's Handbook: Defending Database Servers". Wiley. 2005-07-14.

David Litchfield. "The Oracle Hacker's Handbook: Hacking and Defending Oracle". Wiley. 2007-01-30.

Microsoft. "SQL Injection". December 2008. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>.

Microsoft Security Vulnerability Research & Defense. "SQL Injection Attack". <http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx>.

Michael Howard. "Giving SQL Injection the Respect it Deserves". 2008-05-15.

<http://blogs.msdn.com/sdl/archive/2008/05/15/giving-sql-injection-the-respect-it-deserves.aspx>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	PLOVER		Externally Mined
	7 Pernicious Kingdoms		Externally Mined
	CLASP		Externally Mined

修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Modes of Introduction, Name, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Observed Examples		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Enabling Factors for Exploitation, Modes of Introduction, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name, Related Attack Patterns		

2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description, Name, White Box Definitions		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Potential Mitigations		

相关历史条目

更改日期	相关历史条目
2008-04-11	SQL注入
2008-09-09	无法对进入SQL查询的数据进行消毒处理（即 ‘SQL注入’ ）
2009-01-12	无法对SQL查询内的数据进行消毒处理（即 ‘SQL注入’ ）
2009-05-27	无法保持SQL查询架构（即 ‘SQL注入 ）
2009-07-27	无法保持SQL查询架构（ ‘SQL注入 ）

BACK TO TOP

对SQL命令中使用的特殊元素进行的不正确消毒处理（SQL注入）

Weakness **Status**

ID: 89 (Weakness Base) **:** Draft

描述

简要描述

软件使用来自上游组件,并受外部影响的输入数据构造SQL命令的全部或一部分，但它并没有清洁或者正确清洁特定的元素,当这些元素被SQL
命令使用时,可能会修改SQL命令的本意,从而危及数据库的安全。

扩展描述

如果没有对用户可控的输入数据中的SQL字符串进行充分的验证，那么所生成的SQL查询可能会导致这些输入数据被解释为SQL命令而不是普通用户的输入数据。攻击者就可能对此加以利用来更改查询逻辑,从而绕过安全检查，或插入可以更改后端数据库的额外语句，可能包括执行操作系统命令。

SQL注入已成为数据库驱动网站上常见的问题。这个漏洞很容易被发现，并且容易被利用，因此，即使仅有很小用户的网站或软件包都有可能受到这种攻击。

引入阶段

- 架构与设计阶段
- 实现阶段
- 使用阶段

适用平台

语言

所有

技术类别

数据库服务器

引入模式

这一漏洞通常出现在数据库中保存用户输入的数据丰富的应用程序中。

常见后果

范围	效果
机密性	由于SQL数据库中通常存有敏感数据，因此机密性损失通常是伴随SQL注入漏洞同时存在的问题。

身份认证	如果使用弱SQL命令来检查用户名和密码，那么在就有可能在另一个用户不知道密码的情况下连接到系统中。
授权	如果授权的信息保存在SQL数据库，就有可能通过利用SQL注入的漏洞更改该信息。
完整性	正如有可能读取敏感信息，因此也可以利用SQL注入攻击对此信息进行修改、甚至删除。

被利用的可能性

非常高

被利用的原因

应用程序动态生成包含用户输入的查询。

检测方法

自动静态分析

使用自动静态分析工具通常可以检测到该漏洞。许多现代工具使用数据流分析或约束型技术来减少误报数量。

如果执行的是正确的输入验证，那么自动静态分析就可能无法识别该漏洞，从而导致误报的发生- 即产生没有任何安全后果也不需要修改任何代码的警告。

自动静态分析可能无法检测到是否使用了定制的API函数或间接调用SQL命令的第三方库，从而导致有漏洞未报的情况- 特别是在没有API/库代码供分析的情况下更是这样。

人工分析

人工分析有助于发现这一漏洞，但在有限的时间内可能无法达到预期的代码覆盖率。鉴于攻击面可能过大，所以如果为这一漏洞要考虑所有输入数据，那么操作起来就很困难了。

示例

示例1

2008年，大量Web服务器受到使用相同的SQL注入攻击字符串的损害。这种单一字符串针对许多不同的程序。当时使用 SQL注入来修改网站、服务恶意代码。 [1]

示例2

下面的代码动态地构建并执行搜索匹配指定itemname的SQL查询。要求userName与先前认证通过的用户名相匹配。Itemname与输入itemName.Text相匹配。

(Bad Code)

Example Language: **C#**

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND itemname = '" + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

本代码打算执行的查询遵循：

```
SELECT * FROM items WHERE owner = <userName> AND itemname = <itemName>;
```

但是，由于查询的动态建立是通过连接常量库查询字符串和用户输入的字符串来实现的，因此只有在itemName中不包含单引号字符时，查询才能正确执行。如果用户名为wiley的攻击者输入字符串：

(Attack)

```
name' OR 'a'='a
```

作为itemName，那么查询就会变成：

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

增加的：

(Attack)

```
OR 'a'='a'
```

条件会导致WHERE子句的估值始终为true，因此查询在逻辑上就等同于一个更为简单的查询：

(Attack)

```
SELECT * FROM items;
```

查询的这种简化使攻击者能够绕过查询只返回身份验证合格的用户所拥有的项目的要求；而查询现在所返回的是存储在项目表中的所有条目，不论所有者是谁。

示例3

该示例检查的是前面例子中构建并执行的传递给查询的一个由不同的恶意值所造成的影响有多大。如果用户名为wiley的攻击者输入字符串：

(Attack)

```
name'; DELETE FROM items; --
```

作为itemName，那么该查询就会变成下面两个查询：

(Attack)

Example Language: **SQL**

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
--'
```

许多数据库服务器，其中包括微软(R) SQL Server 2000，都允许被分号分隔的多个SQL语句被同时执行。虽然这种攻击字符串会导致在Oracle和其他不允许批量执行由分号分隔的语句的数据库服务器上执行出错，但在允许分批执行的数据库中，这种类型的攻击仍然允许攻击者对数据库执行任意指令。

应注意尾随的双连字符(--

),其中对大多数的数据库服务器规定，语句的其余部分应被视为一个注释，而不被执行。在这种情况下，注释字符所起的作用是删除被更改的查询所遗留下来的尾随单引号。在这种方法在不允许使用注释的数据库中，使用类似于前例中所示的办法，仍然可以使一般的攻击有效发挥作用。

若攻击者输入字符串

(Attack)

```
name'; DELETE FROM items; SELECT * FROM items WHERE 'a'='a
```

那么就会创建下列三个有效语句：

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
SELECT * FROM items WHERE 'a'='a';
```

一种传统的办法来防止SQL注入攻击就是将它当作一个输入验证问题来处理，要么只接受安全值在白名单中的字符，要么识别并躲开存在潜在恶意值的黑名单。白名单可能是严格执行输入验证规则的一个非常有效的手段，但参数化的SQL语句需要较少的维护，并且能够在安全方面提供更多的保障。黑名单可以说总是充满漏洞，让其无法有效阻止SQL的注入攻击。例如，攻击者可以：

- 找到没被引用的字段
- 设法绕过对于某些避开元字符的需求
- 使用预先写好的存储过程来隐藏注入的元字符

手动将输入数据中的字符转义至SQL查询可以起到帮助的作用，但不能确保应用程序不受SQL注入的攻击。

另一种通常用来处理SQL注入攻击的办法是使用存储过程。虽然存储过程
能够防止某些类型的SQL注入攻击，但还是有许多别的问题防止不了。例如，下面的PL / SQL程序很容易受到和显示在第一个例子中一样的SQL注入攻击。

(Bad Code)

```
procedure get_item ( itm_cv IN OUT ItmCurTyp, usr in varchar2, itm in varchar2)
is open itm_cv for
' SELECT * FROM items WHERE ' || 'owner = '|| usr || ' AND itemname = ' || itm || ';
end get_item;
```

通过限制可以传递给参数的语句的类型，存储过程通常有助于防止SQL注入攻击。然而，仍有很多受限制和有意思的语句绕过存储过程的限制。而且，存储过程可以防止某些漏洞，但不能保证您的应用系统不受SQL注入的攻击。

示例4

MS

SQL具有内置的函数，可以执行shell命令。这种情况中的SQL注入可能是灾难性的。例如，下面表单的查询：

(Bad Code)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='$user_input' ORDER BY PRICE
```

在这里，$user_input 来自于用户，并且没有经过过滤。

如果用户提供的字符串是:

(Attack)

```
' exec master..xp_cmdshell 'vol' --
```

那么查询就会遵循下列形式: "

(Attack)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='' exec master..xp_cmdshell 'vol' --' ORDER BY PRICE
```

现在，此查询可分为:

- [1]第一个SQL查询：SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY=''
- [2]第二个SQL查询，执行一个shell命令：exec master..xp_cmdshell 'vol'
- [3]一个MS SQL注释： --' ORDER BY PRICE

可以看出，恶意输入可以将一个查询的语义变为一个查询、一个shell命令的执行以及注释。

示例5

代码计划根据一个消息ID打印该消息的摘要。

(Bad Code)

Example Language: **PHP**

```
$id = $_COOKIE["mid"];
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

程序员可能假设攻击者无法修改cookie而跳过$输入验证。不过，处理自定义客户端代码或甚至在Web浏览器中都很容易实现。

尽管$ id包裹在以对mysql_query调用的单引号中，但攻击者仍可以将传入的mid cookie简单地变成：

(Attack)

```
1432' or '1' = '1
```

结果将产生查询：

(Result)

```
SELECT MessageID, Subject FROM messages WHERE MessageID = '1432' or '1' = '1'
```

这不仅会检索消息编号1432，还会检索所有其他消息。

在这种情况下，程序员可以对代码进行简单的修改从而消除SQL注入：

(Good Code)

Example Language: **PHP**

```
$id = intval($_COOKIE["mid"]);
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

但，如果该代码旨在支持含有不同消息框的多个用户，那么代码可能还需要进行访问控制检查（CWE-285），来确保应用程序用户有权查看该消息。

示例6

本示例试图获得用户提供的最终名称，并将该名称输入到数据库中。

(Bad Code)

Example Language: **Perl**

```
$userKey = getUserID();
$name = getUserInput();
# ensure only letters, hyphens and apostrophe are allowed
$name = whiteList($name, "^a-zA-z'-$");
$query = "INSERT INTO last_names VALUES('$userKey', '$name')";
```

尽管程序员对用户输入使用了白名单，但这也有缺点。首先，用户仍可以提供在SQL中被作为注释结构的连字符。如果用户进行指定-

那么该语句的其余部分将被视为注释，从而可能会绕过安全逻辑。此外，白名单允许同是SQL中命令分隔数据的单引号。如果用户提供了一个带有撇号的名称，那么就可能能够改变整个语句的结构，甚至改变程序控制流，可能对机密信息进行访问或修改。在这种情况下，单引号和撇号都是用于最终名称的合法字符，必须进行允许操作。相反，程序员可能想使用准备好的语句或对输入数据进行编码程序，从而防止任何数据/指令误解。

已发现的示例

参考	描述
CVE-2004-0366	链：用于数据库认证的库中SQL注入允许SQL注入和绕过认证。
CVE-2008-2790	通过本应是数字标识的SQL注入。
CVE-2008-2223	通过本应是数字标识的SQL注入。
CVE-2007-6602	通过用户名称的SQL注入。
CVE-2008-5817	通过用户名称或密码字段的SQL注入。
CVE-2003-0377	使用精心制作的组名称现安全产品中进行SQL注入。

CVE-2008-2380	向认证库中进行SQL注入。

可能的漏洞消除办法

阶段：架构与设计阶段

策略：使用库或框架

使用不允许该漏洞出现或能够提供可以使本漏洞更容易被避免的已经审查的库或框架。

例如，应考虑使用Hibernate或Enterprise Java Beans等持久层，这样可以较有效地抵御SQL，如果使用得当的话。

阶段：架构与设计阶段

策略：参数化处理

如果可以，使用可自动执行数据与代码分离的结构化机制。这些机制可能能够进行相关的报价、编码、并自动验证，而不是依赖开发人员在每一个有输出数据生成的地方发挥作用。

使用预处理语句、参数化查询或已经参数化的存储过程来处理SQL查询。这些功能须能够接受参数或变量并支持强类型。

```
String userName = ctx.getAuthenticatedUserName();
String itemName = request.getParameter("itemName");
String query = "SELECT * FROM items WHERE itemname=? AND owner=?";
Query stmt = sess.createQuery(query);
stmt.setString(0, itemName);
stmt.setString(1, userName);
List items = stmt.list();
```

不要在这些功能内部使用“exec”或类似功能来动态地构建和执行查询字符串，因为这样您可能又重新引入了SQL注入。

阶段：架构与设计阶段

遵循最低权限原则去创建SQL数据库的用户帐户。该数据库用户应仅拥有使用其帐户所需要的最低权限。如果系统要求显示用户可以读取并修改自己的数据，那么应限制他们的权限，让他们不能读/写别人的数据。尽可能对所有数据库对象使用最严格的权限，如对已存储进程仅有执行权限。

阶段：架构与设计阶段

对于在客户端执行的任何安全检查，应确保这些检查是在服务器端再做一次，以避免CWE-602漏洞。攻击者可通过在检查完成后修改值或通过更改客户端从而完全删除客户端检查来绕过客户端检查。然后，这些修改后的值将被提交给服务器。

阶段：实现阶段

如果无论有什么样的风险，您都需要使用动态生成的查询字符串，那么应使用正确的编码和输入转义。不要建立自己的实现，因为这样的功能可能会在数据库或编程语言中找到。例如，Oracle

DBMS_ASSERT包可以检查或加强参数所具有的使它们不易受到SQL注入攻击的某些特性。对于MySQL，在C和PHP中都可以找到mysql_real_escape_string() API函数。

阶段：实现阶段

策略：输入验证

假定所有输入都是恶意的。使用“接受已知良好”的输入验证策略，即使用严格符合规格的可接受输入的白名单。拒绝不完全符合规格的所有输入，或将其转化为完全符合规格的情况。不要单纯依赖对于恶意或有缺陷输入（即不要依赖黑名单）的查找。但，黑名单可用于检测潜在攻击或者确定哪些输入有缺陷应该被断然拒绝。

当执行输入验证时，应考虑所有可能的相关属性，包括长度、输入类型、可接受值的范围、丢失或额外输入、语法、相关领域的连贯性以及业务规则的符合程序。以业务规则逻辑为例，“boat”可能语法上是有效的，因为它仅包含字母数字字符，但如果您期待颜色如“红色”或“蓝色”之类的信息，它就是无效的。

当构建SQL查询字符串时，应使用可以对根据请求中预期参数值设置的字符串进行严格限制的白名单。这将间接地限制攻击范围，但这种技术没有正确的输出编码和转义更重要。

请注意，尽管输入验证可能会提供一些纵深??防御，但正确的输出编码、转义和引用仍是防止SQL注入最有效的解决方案。这是因为它们可以有效地限制输出数据中会出现的内容。输入验证做不到百分之百阻止SQL注入，特别是当您需要支持可能包含任意字符的自由格式文本字段的时候。例如，名称“O'Reilly”很可能会通过验证，因为这是一个常见的英文姓氏。但，它不能被直接插入到数据库中，因为它包含了“'”撇号字符，这就将需要进行转义或以其他方式处理。在这种情况下，去除撇号可能会降低SQL注入风险，但这会产生不正确的行为，因为所记录的名字就是错误的了。

在可行的情况下，完全禁止元字符而不是对其进行转义可能是最安全的作法。这种作法会提供一些深入防御。在数据被输入数据库以后，后来进程在使用元字符之前可能忘记对其进行转义，而您也可能无法控制这些进程。

阶段：测试、实现阶段

使用针对这种漏洞类型的自动静态分析工具。许多现代技术都是使用数据流分析来尽量降低误报。但由于不可能达到100%的准确率和覆盖率，所以这并不是一个完美的解决方案。

阶段：测试阶段

使用动态的利用大型测试套件处理多种输入的与软件互动的工具和技术，如模糊测试（fuzzing）、坚固性测试、故障注入。软件的操作可以被放缓，但它不应不稳定、崩溃或产生不正确的结果。

阶段：使用阶段

使用可以检测到攻击此漏洞的应用程序防火墙。这可能无法捕捉所有的攻击，而且可能需要进行一些定制工作。但是，在代码无法被修复的情况下（由于代码受第三方控制），在应用更为全面的软件安全保护措施的同时，作为一种紧急事件的预防措施，或用作纵深防御，这种作法都是有益的。

关系

性质	类型	ID	名称	
ChildOf		20	Improper Input Validation	**700**
ChildOf		77	Improper Sanitization of Special Elements used in a Command ('Command Injection')	**699** **1000**
ChildOf		713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**629**
ChildOf		722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	711
ChildOf		727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**711**
ChildOf		751	2009 Top 25 - Insecure Interaction Between Components	**750**
ChildOf		801	2010 Top 25 - Insecure Interaction Between Components	**800**
ParentOf		564	SQL Injection: Hibernate	**699** **1000**
MemberOf		630	Weaknesses Examined by SAMATE	**630**
MemberOf		635	Weaknesses Used by NVD	**635**
CanFollow		456	Missing Initialization	1000

关联说明

SQL注入可能是由于特殊字符管理不善、MAID或黑名单/白名单问题造成的。是首要的身份验证错误。

缺陷类别映射

映射分类	节点	适用于	映射节点名称
PLOVER			SQL injection
7 Pernicious Kingdoms			SQL Injection
CLASP			SQL injection
OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws
WASC	19		SQL Injection

相关的攻击模式

CAPEC-ID	攻击模式名称	*(CAPEC Version: 1.5)*
7	SQL盲注	
66	SQL注入	
108	通过SQL注入执行命令行	

109	对象关系映射注入
110	通过SOAP参数篡改进行SQL注入

白盒定义

通过SOAP参数篡改进行SQL注入

1. 起始语句接受输入

2. 结束语句执行SQL命令，在以下情况下：

a. 输入为SQL命令的一部分

b. 输入中包含SQL句法（尤其是存在有查询分隔符的情况下）

参考

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 1: SQL Injection." Page 3. McGraw-Hill. 2010.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 12, "Database Input Issues" Page 397. 2nd Edition. Microsoft. 2002.

OWASP. "SQL Injection Prevention Cheat Sheet". <http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>.

Steven Friedl. "SQL Injection Attacks by Example". 2007-10-10. <http://www.unixwiz.net/techtips/sql-injection.html>.

Ferruh Mavituna. "SQL Injection Cheat Sheet". 2007-03-15. <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>.

David Litchfield, Chris Anley, John Heasman and Bill Grindlay. "The Database Hacker's Handbook: Defending Database Servers". Wiley. 2005-07-14.

David Litchfield. "The Oracle Hacker's Handbook: Hacking and Defending Oracle". Wiley. 2007-01-30.

Microsoft. "SQL Injection". December 2008. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>.

Microsoft Security Vulnerability Research & Defense. "SQL Injection Attack". <http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx>.

Michael Howard. "Giving SQL Injection the Respect it Deserves". 2008-05-15.

<http://blogs.msdn.com/sdl/archive/2008/05/15/giving-sql-injection-the-respect-it-deserves.aspx>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	PLOVER		Externally Mined
	7 Pernicious Kingdoms		Externally Mined
	CLASP		Externally Mined

修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Modes of Introduction, Name, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Observed Examples		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Enabling Factors for Exploitation, Modes of Introduction, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name, Related Attack Patterns		

2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description, Name, White Box Definitions		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Potential Mitigations		

相关历史条目

更改日期	相关历史条目
2008-04-11	SQL注入
2008-09-09	无法对进入SQL查询的数据进行消毒处理（即 ‘SQL注入’ ）
2009-01-12	无法对SQL查询内的数据进行消毒处理（即 ‘SQL注入’ ）
2009-05-27	无法保持SQL查询架构（即 ‘SQL注入 ）
2009-07-27	无法保持SQL查询架构（ ‘SQL注入 ）

BACK TO TOP

Failure to Preserve Web Page Structure ('Cross-site Scripting')

Weakness **Status:** Usable

ID: 79 (Weakness Base)

描述

简要描述

该软件没有对用户可控的输入数据进行充分验证、过滤、避免和/或Encode，就将其放在输出数据中，用于WEB页面服务于其他用户。

扩展描述

当下列情况发生时，出现跨站脚本（XSS）漏洞：

1. 非信任的数据进入Web应用程序中，这样的数据通常来自于Web请求。

2. Web应用程序动态生成一个包含该非信任数据的网页。

3.
在页面生成过程中，应用程序没有阻止数据去包含Web浏览器可执行的内容，如JavaScript、HTML标记、HTML属性、鼠标事件、Flash、ActiveX等。

4. 受害者通过Web浏览器访问生成的网页，其中包含使用非信任数据所注入的恶意脚本。

5.
由于该脚本来自于Web服务器所发送网页，因此受害者的Web浏览器是在Web服务器的域范围内执行恶意脚本。

6.
这从本质上违背了Web浏览器相同来源策略的意图，该策略规定，在一个域中的脚本不应能在不同域够中访问资源或运行代码。

主要有三种类型的跨站脚本：

类型1：反射类XSS（或非持久XSS）

服务器直接从HTTP请求读取数据，并将其反射在HTTP响应中。当攻击者诱使受害者向脆弱的Web应用程序提供危险内容时，就会发生反射XSS攻击，然后反射回受害者，并通过Web浏览器执行。提供恶意内容最常见的机制是将该内容作为一个参数包含在公开发送给或直接通过邮件发送给受害者的URL中。以这种方式构造的URL构成了众多的钓鱼计划的核心，使攻击者能够说服受害者访问引向脆弱网站的网址。在该网站将攻击者的内容反射回被攻击者后，该内容就会被受害者的浏览器所执行。

类型2：存储类XSS（或持续XSS）

应用程序在数据库、消息论坛、访客日志或其它可信的数据存储中存储危险数据。该危险数据随后被读回到应用程序，并被包含在动态内容中。从攻击者的角度看，注入恶意内容的最佳位置是能够展示

给众多用户的区域或是展示给特别用户的区域。特定的用户通常都具有应用程序中的较高权限，或能够接触到对攻击者有价值的敏感数据。如果这样的用户执行恶意内容，那么攻击者就可能可以代表该用户执行特权操作或获取属于该用户的访问敏感数据的权力。例如，攻击者可能会向日志消息中注入XSS，但在管理员查看该日志的时候，可能并没有对其进行妥善处理。

类型0：基于DOM的XSS攻击

在基于DOM的XSS攻击中，客户端将XSS注入到页面中;在其他类型中是由服务器执行注入。基于DOM的XSS一般涉及被发送给客户的、受服务器控制的、值得信赖的脚本，如JavaScript，在客户提高表单之前，JavaScript对该表单执行安全检查。如果服务器提供的脚本处理用户提供的数据，然后将数据注入到网页中（如动态HTML），那么就可能发生基于DOM的XSS攻击。

一旦恶意脚本被注入，攻击者就可以执行各种恶意活动了。攻击者可能会将其中可能包括会话信息cookie之类的私人信息从受害者的机器转移到攻击者机器上。攻击者可以代表受害者向网站发送恶意请求，如果受害者具有管理该网站的管理员权限，那么这种作法对于该网站是尤其危险的。网络钓鱼攻击可以用来模拟信任网站，诱骗受害者输入密码，让攻击者能够危及受害人在该网站上的帐户。最后，该脚本还可能Web浏览器本身的漏洞，从而接管受害者的机器，这种操作有时也被称为“黑客操作”。

在多数情况下，受害者可能根本意识不到受到攻击。面对细心的用户，攻击者经常使用多种方法来对攻击的恶意部分进行编码，如URL编码或Unicode，这样让请求看起来不太可疑。

其它称谓

XSS

CSS: “CSS”曾被作为该漏洞的缩写，但这一缩写会引起与“层叠样式表”之间的混淆，所以对于该缩写的使用已大为下降。

引入阶段

- 架构与设计阶段
- 实现阶段

适用平台

语言

语言无关性

架构范例

基于Web的：*（常用）*

技术类

Web-Server: *（常用）*

平台注释

由于需要进行大量的开发训练才能避免XSS漏洞，因此该漏洞在web应用程序中非常常见。

常见后果

范围	效果
机密性	由跨站脚本造成的最常见攻击一般为披露存储在用户cookie的信息。通常情况下，恶意用户会创建一个客户端脚本，在网络浏览器对其进行分析时，该脚本会执行某些活动（例如向某一E-mail地址发送所有网站的Cookie）。该脚本就会被加载，并且每一个访问该网站的用户都会对它进行运行。由于要求运行该脚本网站可以访问有问题的Cookie，因此恶意脚本也可以对其进行访问。
访问控制	在某些情况下，当跨站点脚本与其他漏洞同时存在时，有可能在受害者的计算机上运行任意代码。
机密性完整性可用性	无论是存储型还是反射型，XSS攻击的后果都是一样的。其不同之处在于有效载荷如何到达服务器。 XSS攻击可能会给最终用户带很各种麻烦，其严重程度从产生困扰直到毁掉整个帐户。某些跨站脚本漏洞可以被利用来操纵或窃取cookie，创建有效用户可能被误认为正确的请求，损坏机密信息，或出于不可各种不可告人的目的，在最终用户系统上执行恶意代码。其它破坏性攻击还包括披露最终用户的信息文件，安装木马程序，将用户重定向到其他页面或网站，（在Microsoft Internet Explorer中）运行来自用户认为可信网站上的“Active X”控件，并修改介绍的内容。

被利用的可能性

高到非常高

被利用的原因

跨站脚本攻击可能出现在所有恶意用户被允许向可信网站发布未经校准的材料，让其它有效用户使用，这些常见的地方包括提供基于Web邮件列表样式功能的公告板网站等。

存储类XSS攻击最开始是始于向访客提供“留言”功能的网站。攻击者将JavaScript包含在其留言簿条目中，之后所有访问该留言页的访客都会执行这一恶意代码。如上述示例所显示，XSS漏洞是由在HTTP响应中包含有未经验证数据的代码所引起的。

检测方法

自动静态分析

使用针对这种类型漏洞的自动静态分析工具。许多现代技术都使用数据流分析，来最大限度地减少误报数量。其实这并不是一个完美的解决方案，因为100%的准确率和覆盖率是无法实现的，尤其在涉及到多个组件的时候。

效率：中等

黑盒子方法

使用XSS欺骗表单[REF-14]或自动测试生成工具帮助攻击者发动针对您Web应用程序的多种攻击。该欺骗表单中包含了许多微妙的专门针对XSS防御薄弱系统的XSS变化形式。

效率：中等

关于存储类XSS攻击，由数据存储所造成的间接会导致更加难以发现问题。测试人员必须首先向数据存储中注入XSS字符串，然后找到可以发送XSS字符串到程序其它用户的合适的应用程序功能。这是两个不同的步骤，其中在XSS被最初注入到数据存储中以后，XSS攻击的激活可能需要分钟、几小时甚至几天。

示例

示例1

该示例中涵盖了反射类XSS（类型1）的情况。

下面的JSP代码段从HTTP请求中读取了一个员工ID、eid，并将其显示给用户。

(Bad Code)

Example Language: **JSP**

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID: <%= eid %>
```

下列ASP.NET代码段从HTTP请求中读取了一个员工ID，并将其显示给用户。

(Bad Code)

Example Language: **ASP.NET**

```
...
protected System.Web.UI.WebControls.TextBox Login;
protected System.Web.UI.WebControls.Label EmployeeID;
...
EmployeeID.Text = Login.Text;
... (HTML follows) ...
<p><asp:label id="EmployeeID" runat="server" /></p>
...
```

如果员工ID变量只包含标准的字母数字文本，那么在本示例中的代码就可以正常运行。如果其中含有包含元字符或源代码的值，那么该代码在显示HTTP响应的同时就会被Web浏览器执行。最初，可能显现出来的并不像一个漏洞。但，为什么会有人输入一个会导致自己的计算机上运行恶意代码的网址呢？其真正的危险是，攻击者会创建恶意的URL，然后使用电子邮件或社会工程技巧，引诱受害者访问URL链接。当受害者点击该链接时，他们就会不知不觉地通过脆弱的Web应用程序将恶意内容反射到自己的电脑中了。

示例2

该示例中涵盖了反射类XSS（类型2）的情况。

下列JSP代码段使用给定的ID查询员工数据库，并打印出相应的员工姓名。

(Bad Code)

Example Language: **JSP**

```
<%
```

```
...
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("select * from emp where id="+eid);
if (rs != null) {
rs.next();
String name = rs.getString("name");
%>

Employee Name: <%= name %>
```

下列ASP.NET代码段使用给定的ID查询员工数据库，并根据该ID打印出相应的员工姓名。

(Bad Code)

Example Language: **ASP.NET**

```
protected System.Web.UI.WebControls.Label EmployeeName;
...
string query = "select * from emp where id=" + eid;
sda = new SqlDataAdapter(query, conn);
sda.Fill(dt);
string name = dt.Rows[0]["Name"];
...
EmployeeName.Text = name;
```

该代码看起来可能并不危险，因为name的值是从数据库读取的，其内容显然受应用程序的管理。但是，如果name的值来源于用户提供的数据，那么数据库就可能成为提供恶意内容的渠道。如果不对存储在数据库中的所有数据进行正确的输入验证，那么攻击者就可能在用户的Web浏览器中执行恶意命令。

已发现示例

参考	描述
CVE-2008-5080	Chain: protection mechanism failure allows XSS
CVE-2006-4308	Chain: only checks "javascript:" tag
CVE-2007-5727	Chain: only removes SCRIPT tags, enabling XSS
CVE-2008-5770	Reflected XSS using the PATH INFO in a URL
CVE-2008-4730	Reflected XSS not properly handled when generating an error message
CVE-2008-5734	Reflected XSS sent through email message.
CVE-2008-	Stored XSS in a security product.

0971	
CVE-2008-5249	Stored XSS using a wiki page.
CVE-2006-3568	Stored XSS in a guestbook application.
CVE-2006-3211	Stored XSS in a guestbook application using a javascript: URI in a bbcode img tag.
CVE-2006-3295	Chain: library file is not protected against a direct request (CWE-425), leading to reflected XSS.

可能的漏洞的消除办法

阶段：架构与设计阶段

策略：库或框架

使用经过审批的库或框架，不允许该漏洞出现或能够提供可以更容易避免这一漏洞的架构。

现有若干有关库和框架可以更容易生成编码正确的输出数据的示例，其中包括微软的反XSS库、OWASP的ESAPI编码模块和Apache Wicket等。

阶段：实现阶段；架构与设计阶段

了解您数据将被使用的环境以及需要进行的编码。当需要在不同组件之间传递数据时，或像网页或多部分邮件消息等在生成的输出数据中同时包含有多个编码时，这一点就显得尤为重要。所有的研究都期望通信协议和数据表示能够确定所需的编码策略。

对于可能成为另一网页输出数据的任何数据来说，尤其是对于通过外部输入数据接收到的数据来说，应针对所有的非字母数字字符进行适当的编码。

同一输出文件不同部分可能需要进行不同的编码，其不同取决于输出数据存在于下列哪个部分：

- HTML正文
- 元素的属性（如SRC = “XYZ” ）
- URIs
- JavaScript部分
- 层叠样式表和样式属性，等。

请注意，HTML实体编码只适用于HTML正文。

咨询XSS Prevention Cheat Sheet[REF- 16]，获取更多有关编码和转义的细节。

阶段：架构与设计阶段

对于客户端上执行的所有安全检查，应确保这些检查在服务器端再次执行，来避免CWE-602的出现。攻击者可以通过在检查后修改值，或更改客户端完全删除客户端检查，来绕过客户端的

检查。然后，这些修改后的值将被提交给服务器。

阶段：实现阶段

使用并指定像ISO- 8859 -1或UTF –
8这样的较强字符编码。如果对编码进行指定，那么Web浏览器就可以猜测网页实际上使用的编码来选择不同的编码。这样您就可能受到与该编码相关的微妙的XSS攻击。参见 CWE-
116来了解更多的编码/转义信息。

阶段：实现阶段

使用Struts，您应将bean的过滤属性设置为true，然后再编写该表单bean的所有数据。

阶段：实现阶段

为了消除针对用户会话cookie的XSS攻击，将会话cookie设置为HttpOnly。在支持HttpOnly功能（如较新版本的Internet
Explorer和Firefox）的浏览器中，该属性可以阻止使用document.cookie的恶意客户端脚本对于用户会话cookie的访问。但由于关不是所有的浏览器都支持HttpOnly，所以这并不是一个完整的解决方案。更重要的是，XMLHttpRequest和其他强大的浏览器技术允许对HTTP标头的读取访问，包括对HttpOnly标志进行设置的Set – Cookie header。

阶段：实现阶段

策略：输入验证

假定所有输入都是恶意的。使用“接受已知良好”的输入验证策略，即使用严格符合规格的可接受输入的白名单。拒绝不完全符合规格的所有输入，或将其转化为完全符合规格的情况。不要单纯依赖对于恶意或有缺陷输入（即不要依赖黑名单）的查找。但，黑名单可用于检测潜在攻击或者确定哪些输入有缺陷应该被断然拒绝。

当执行输入验证时，应考虑所有可能的相关属性，包括长度、输入类型、可接受值的范围、丢失或额外输入、语法、相关领域的连贯性以及业务规则的符合程序。以业务规则逻辑为例，“boat”可能语法上是有效的，因为它仅包含字母数字字符，但如果您期待颜色如“红色”或“蓝色”之类的信息，它就是无效的。

当动态构建网页时，应使用可以对根据请求中预期参数值设置的字符串进行严格限制的白名单。应对所有的输入数据进行验证和清洗，不仅仅是针对用户须指定的那些参数，而且针对请求中的所有数据，包括隐藏字段、cookie、header、URL本身，等等。可能导致持续XSS漏洞的一个常见??错误是只对那些需要被网站反复演示的字段进行验证。我们经常可以看到来自由应用程序服务器所反射请求的数据，或来自于开发团队事先没有预料到的应用程序。此外，未受到充分反射的字段可能被用于未来的开发过程。因此，我们建议对HTTP请求的所有部分进行验证。

请注意，尽管输入验证可能会提供一些纵深??防御，但正确的输出编码、转义和引用仍是防止XSS漏洞最有效的解决方案。这是因为它们可以有效地限制输出数据中会出现的内容。输入验证做不到百分

之百阻止XSS漏洞，特别是当您需要支持可能包含任意字符的自由格式文本字段的时候。例如，在一个聊天应用程序中，因为心表情符号（ “<3” ）很常用，所以很可能会通过验证步骤。但是，它不能被直接插入到网页中，因为其中包含有“<”字符，这将需要进行转义或进行其它处理。在这种情况下，去掉“<”可能会降低XSS风险，但因为表情符号不会被记录下来，所以这样做会产生不正确行为。这看起来会带来一个小小的不便，但，在想要展示不等式的数学论坛中就非常重要了。

即使您在验证过程中犯了一个错误在验证（如忘记1/100的输入字段），适当的编码仍然可能保护您不受注入式攻击。只要输入验证不是孤立进行的，就仍然是一项有用的技术，因为它可以显着降低攻击面，让您能够发现攻击并获得正确编码所不提供的其它安全优势。

一定要在应用程序的明确界面上执行输入验证。这将有助于保护应用程序，即使在某一个数据被重复使用或被移至别处的情况下也是这样。

阶段：使用阶段

使用可以检测攻击该漏洞的应用程序防火墙。这可能无法捕捉到所有的攻击，而且，可能需要进行大量的定制工作。但，在全面的软件安全措施都已部署的情况下，如果代码无法修复（由于受到第三方控制），那么作为一项紧急预防措施这样做就是很有意义的，这样做也有助于提供纵深防御。

详细背景信息

同源策略

同源策略规定，浏览器应该对在可以接触到与客户端网站相关的资源的某一特定网站、或“来源”上运行脚本所能访问的资源进行限制，这一网站或“来源”不应是任何网站或“来源”的客户端资源。该策略旨在阻止网站被修改或读取无关网站的内容。由于万维网涉及许多网站之间的相互作用，因此浏览器必须要执行该策略。

域名

在指XSS攻击时，一个网站的域名大致相当于在该连接的客户一端相关的资源。也就是说，域可以被认为是浏览器存储的用地用户与该网站互动的所有资源。

漏洞出现的次序

次序	描述
结果性漏洞	*（该漏洞的出现取决于其它漏洞是否存在）*

关系

性质	类型	ID	名称		
ChildOf		20	Improper Input Validation	**700**	
ChildOf		74	Failure to Sanitize Data into a Different Plane ('Injection')	**699** **1000**	
ChildOf		442	Web Problems	699	
ChildOf		712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	**629**	

ChildOf		722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	711	
ChildOf		725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	**711**	
ChildOf		751	2009 Top 25 - Insecure Interaction Between Components	**750**	
ChildOf		801	2010 Top 25 - Insecure Interaction Between Components	**800**	
CanPrecede		494	Download of Code Without Integrity Check	1000	
PeerOf		352	Cross-Site Request Forgery (CSRF)	1000	
ParentOf		80	Improper Sanitization of Script-Related HTML Tags in a Web Page (Basic XSS)	**699** **1000**	
ParentOf		81	Improper Sanitization of Script in an Error Message Web Page	**699** **1000**	
ParentOf		83	Improper Neutralization of Script in Attributes in a Web Page	**699** **1000**	
ParentOf		84	Failure to Resolve Encoded URI Schemes in a Web Page	**699** **1000**	
ParentOf		85	Doubled Character XSS Manipulations	**699** **1000**	
ParentOf		86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	**699** **1000**	
ParentOf		87	Failure to Sanitize Alternate XSS Syntax	**699** **1000**	
MemberOf		635	Weaknesses Used by NVD	**635**	
CanFollow		113	Failure to Sanitize CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	1000	
CanFollow		184	Incomplete Blacklist	1000	692

f 成因性质

明示

缺陷类别映射

映射分类	节点	适用于	映射节点名称
PLOVER			Cross-site scripting (XSS)
7 Pernicious Kingdoms			Cross-site Scripting
CLASP			Cross-site scripting
OWASP Top Ten 2007	A1	Exact	Cross Site Scripting (XSS)

OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A4	Exact	Cross-Site Scripting (XSS) Flaws
WASC	8		Cross-site Scripting

相关的攻击模式

CAPEC-ID	攻击模式名称	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
85	Client Network Footprinting (using AJAX/XSS)	
86	Embedding Script (XSS) in HTTP Headers	
32	Embedding Scripts in HTTP Query Strings	
18	Embedding Scripts in Nonscript Elements	
19	Embedding Scripts within Scripts	
63	Simple Script Injection	
91	XSS in IMG Tags	
106	Cross Site Scripting through Log Files	
198	Cross-Site Scripting in Error Pages	
199	Cross-Site Scripting Using Alternate Syntax	
209	Cross-Site Scripting Using MIME Type Mismatch	
243	Cross-Site Scripting in Attributes	
244	Cross-Site Scripting via Encoded URI Schemes	
245	Cross-Site Scripting Using Doubled Characters, e.g. %3C%3Cscript	
246	Cross-Site Scripting Using Flash	
247	Cross-Site Scripting with Masking through Invalid Characters in Identifiers	

参考

[REF-15] Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager and Seth Fogie. "XSS Attacks". Syngress. 2007.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 2: Web-Server Related Vulnerabilities (XSS, XSRF, and Response Splitting)." Page 31. McGraw-Hill. 2010.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 3: Web-Client Related Vulnerabilities (XSS)." Page 63. McGraw-Hill. 2010.

"Cross-site scripting". Wikipedia. 2008-08-26. <http://en.wikipedia.org/wiki/Cross-site_scripting>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 13, "Web-Specific Input Issues" Page 413. 2nd Edition. Microsoft. 2002.

[REF-14] RSnake. "XSS (Cross Site Scripting) Cheat Sheet". <http://ha.ckers.org/xss.html>.

Microsoft. "Mitigating Cross-site Scripting With HTTP-only Cookies". <http://msdn.microsoft.com/en-us/library/ms533046.aspx>.

Mark Curphey, Microsoft. "Anti-XSS 3.0 Beta and CAT.NET Community Technology Preview now Live!". <http://blogs.msdn.com/cisg/archive/2008/12/15/anti-xss-3-0-beta-and-cat-net-community-technology-preview-now-live.aspx>.

"OWASP Enterprise Security API (ESAPI) Project". <http://www.owasp.org/index.php/ESAPI>.

Ivan Ristic. "XSS Defense HOWTO". <http://blog.modsecurity.org/2008/07/do-you-know-how.html>.

OWASP. "Web Application Firewall". <http://www.owasp.org/index.php/Web_Application_Firewall>.

Web Application Security Consortium. "Web Application Firewall Evaluation Criteria". <http://www.webappsec.org/projects/wafec/v1/wasc-wafec-v1.0.html>.

RSnake. "Firefox Implements httpOnly And is Vulnerable to XMLHTTPRequest". 2007-07-19.

"XMLHttpRequest allows reading HTTPOnly cookies". Mozilla. <https://bugzilla.mozilla.org/show_bug.cgi?id=380418>.

"Apache Wicket". <http://wicket.apache.org/>.

[REF-16] OWASP. "XSS (Cross Site Scripting) Prevention Cheat Sheet". <http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet>.

相关历史信息

提交			
提交日期	**提交人**	**公司**	**来源**
	PLOVER		Externally Mined
修改			
修改日期	**修改人**	**公司**	**来源**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Description, Relationships, Other Notes, References, Taxonomy Mappings, Weakness Ordinalities		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Background Details, Common Consequences, Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Description		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Observed Examples, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Detection Factors, Enabling Factors for Exploitation, Observed Examples		
2010-02-	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Detection Factors, Potential		

16	Mitigations, References, Relationships, Taxonomy Mappings		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Description, Potential Mitigations, Related Attack Patterns		

相关历史条目

更改日期	相关历史条目
2008-04-11	跨站脚本 (XSS)
2009-01-12	未能对网页中的指令进行消毒（即“跨站脚本攻击”）
2009-05-27	未能维护网页结构（即“跨站脚本”）

BACK TO TOP

扫描语言

语言	哈希数字	改变日期
Java	0711815348928545	2015/2/2
JavaScript	0215495526097913	2015/2/2
VbScript	0349820356141062	2015/2/2